CertyIQ

CertyIQ

Premium exam material

Get certification quickly with the CertyIQ Premium exam material.
Everything you need to prepare, learn & pass your certification exam easily. Lifetime free updates
First attempt guaranteed success.

https://www.CertyIQ.com

About CertyIQ

We here at CertyIQ eventually got enough of the industry's greedy exam paid for. Our team of IT professionals comes with years of experience in the IT industry Prior to training CertIQ we worked in test areas where we observed the horrors of the paywall exam preparation system.

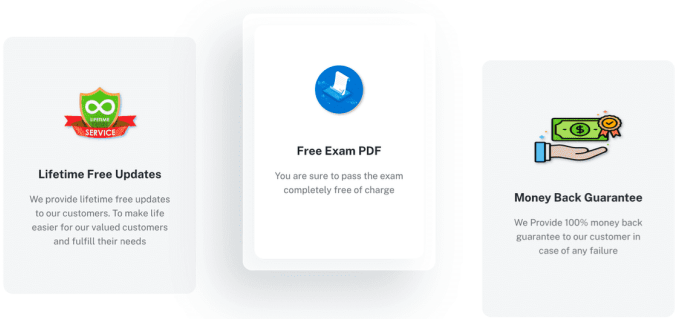
The misuse of the preparation system has left our team disillusioned. And for that reason, we decided it was time to make a difference. We had to make In this way, CertyIQ was created to provide quality materials without stealing from everyday people who are trying to make a living.

Doubt Support

We have developed a very scalable solution using which we are able to solve 400+ doubts every single day with an average rating of 4.8 out of 5.

https://www.certyiq.com

Mail us on - certyiqofficial@gmail.com



John

October 19, 2022

★★★★★

Thanks you so much for your help. I scored 972 in my exam today. More than 90% were from your PDFs!

Dana

September 04, 2022

★★★★★

Thanks a lot for this updated AZ-900 Q&A. I just passed my exam and got 974, I followed both of your Az-900 videos and the 6 PDF, the PDFs are very much valid, all answers are correct. Could you please create a similar video/PDF for DP900, your content/PDF's is really awesome. The team did a really good job. Thank You 😊.

Ahamed Shibly

2 months ago

★★★★★

Customer support is realy fast and helpful, I just finished my exam and this video along with the 6 PDF helped me pass! Definitely recommend getting the PDFs. Thank you!

October 22, 2022

★★★★★

Passed my exam today with 891 marks. Out of 52 questions, 51 were from certyiq PDFs including Contoso case study.
Thank You certyiq team!

Henry Rome

2 months ago

★★★★★

These questions are real and 100 % valid. Thank you so much for your efforts, also your 4 PDFs are awesome, I passed the DP900 exam on 1 Sept. With 968 marks. Thanks a lot, buddy!

Esmaria

2 months ago

★★★★★

Simple easy to understand explanations. To anyone out there wanting to write AZ900, I highly recommend 6 PDF's.Thank you so much, appreciate all your hard work in having such great content. Passed my exam Today - 3 September with 942 score.

Microsoft

(SC-300)

Microsoft Identity and Access Administrator

Total: **309 Questions**

Link: https://certyiq.com/papers/microsoft/sc-300

Question: 1 CertyIQ

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

Answer: B

Explanation:

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.

Question: 2 CertyIQ

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

Answer: A

Explanation:

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)

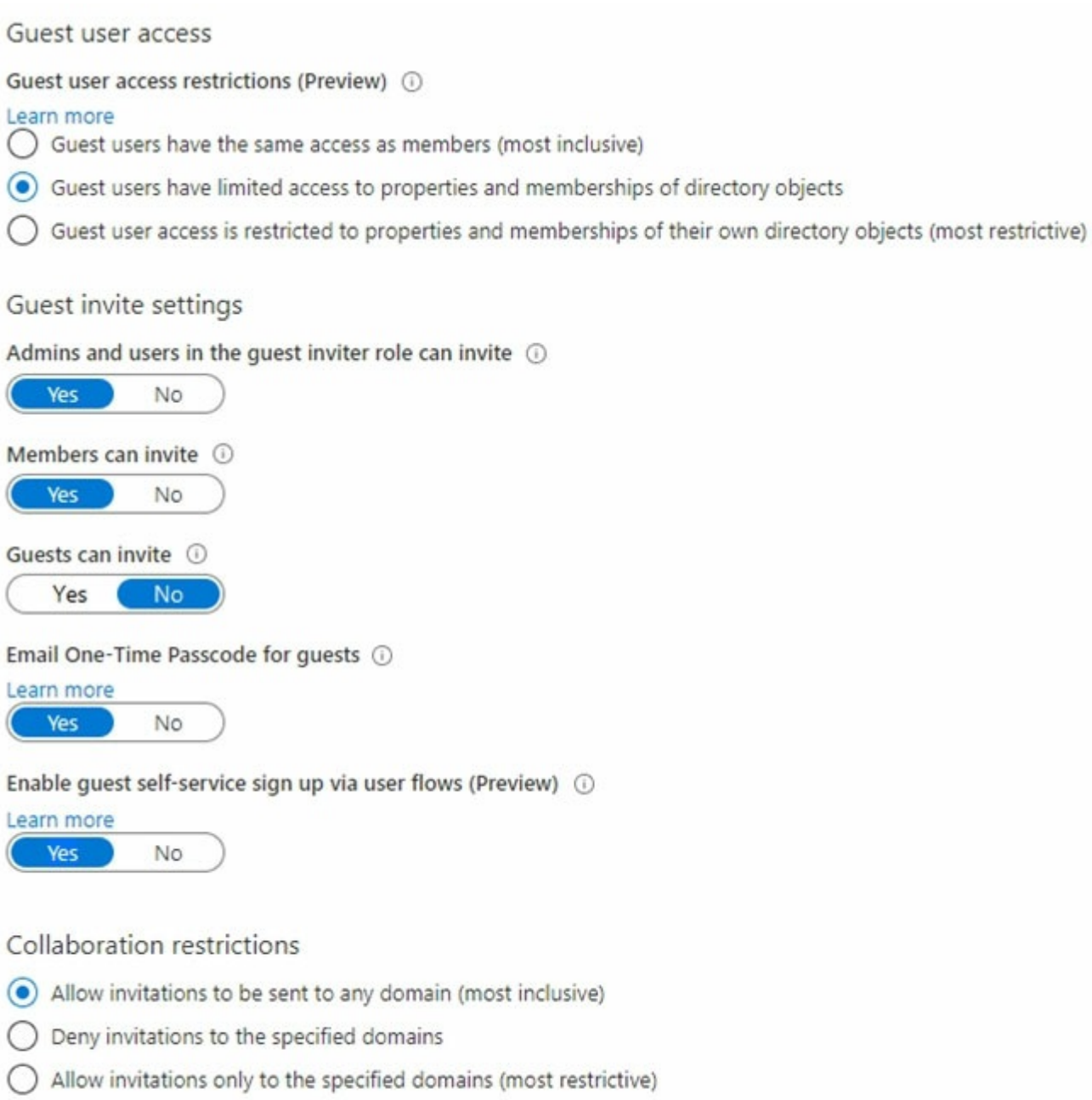
e.g. Set-MsolCompanySettings -AllowEmailVerifiedUsers $false -AllowAdHocSubscriptions $false

Reference:

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

Question: 3 CertyIQ

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.)



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

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

Which users will be emailed a passcode?

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

Answer: A

Explanation:

Correct Answer= A

Here = bsmith@fabrikam.com

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.

Question: 4 CertyIQ

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

Answer: C

Explanation:
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

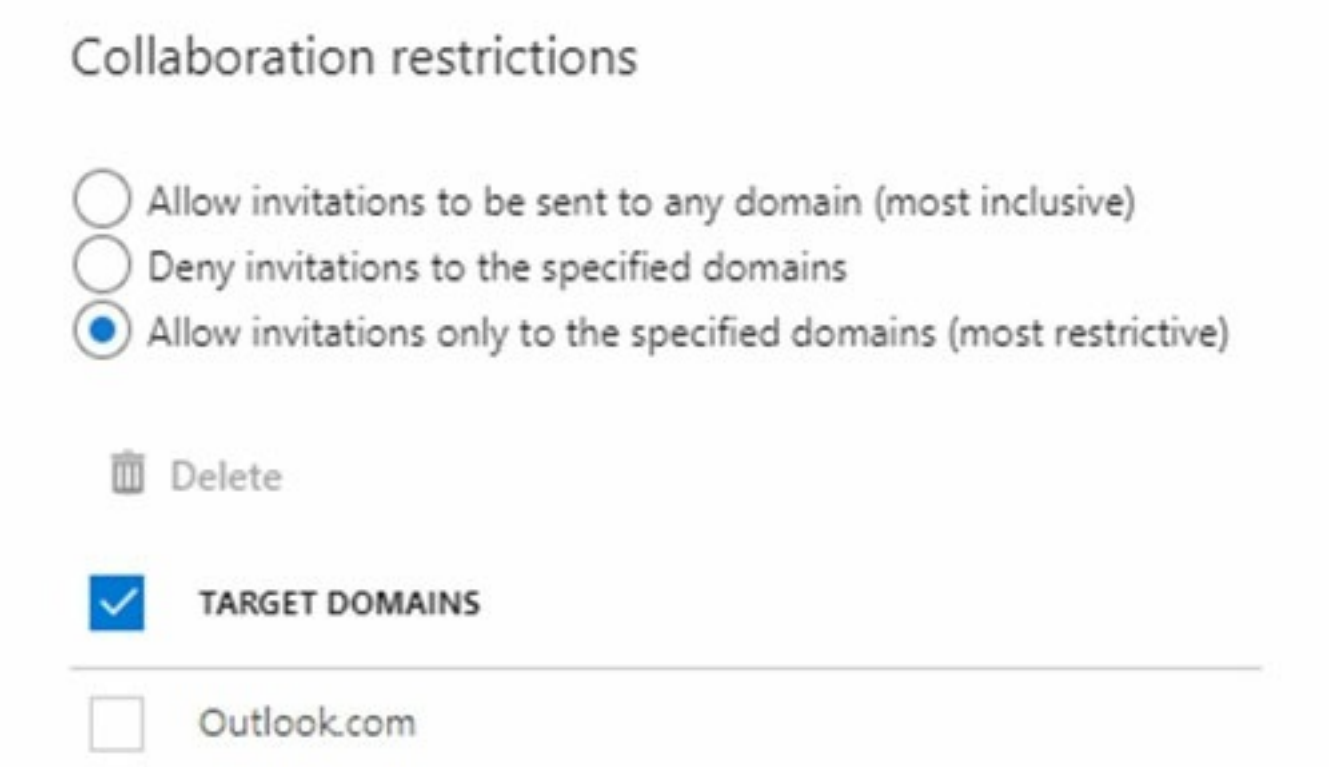
Reference:
https://docs.microsoft.com/en-us/microsoft-365/admin/manage/remove-licenses-from-users?view=o365-worldwide

Question: 5 CertyIQ

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.



From a Microsoft SharePoint Online site, a user invites to the site.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

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

Answer:

Answer Area

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

Explanation:

Here = user3@adatum.com

Box 1: yes.

Box2: yes

Box 3: No

Question: 6 CertyIQ

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

Answer: AB

Explanation:

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

Required values are:

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

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

Reference:

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

Question: 7 CertyIQ

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

Answer: E

Explanation:

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

Tested in Lab environment:

Mail enabled Security Group can only be managed in the M365 Admin Center.

In AAD, you can't modify the membership. - "Some groups can't be managed in the Azure Portal."

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.

Question: 8 CertyIQ

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	Answer Area
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:

Actions	Answer Area
Sign in to the Microsoft 365 admin center.	Create a self-signed user account in the Azure AD tenant.
Create a self-signed user account in the Azure AD tenant.	Sign in to the Microsoft 365 admin center.
From the Microsoft 365 admin center, add the domain name.	Respond to the Become the admin message.
Respond to the Become the admin message.	Create a TXT record in the contoso.com DNS zone.
From the Microsoft 365 admin center, remove the domain name.	
Create a TXT record in the contoso.com DNS zone.	

Explanation:

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

Question: 9 CertyIQ

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:

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

Explanation:

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

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

Reference:

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

Question: 10 CertyIQ

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

Answer: B

Explanation:

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.

Reference:

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

Question: 11 CertyIQ

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

Answer: A

Explanation:

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.

Reference:

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

Question: 12 CertyIQ

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

Answer: B

Explanation:

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

Reference:

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

Question: 13 CertyIQ

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

Answer: B

Explanation:

Because nested group do not inherit licenses.

Reference:

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

Question: 14 CertyIQ

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

Answer: D

Explanation:

In Question, = user1@outlook.com

Reference:

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

Question: 15 CertyIQ

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.

Answer: C

Explanation:

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

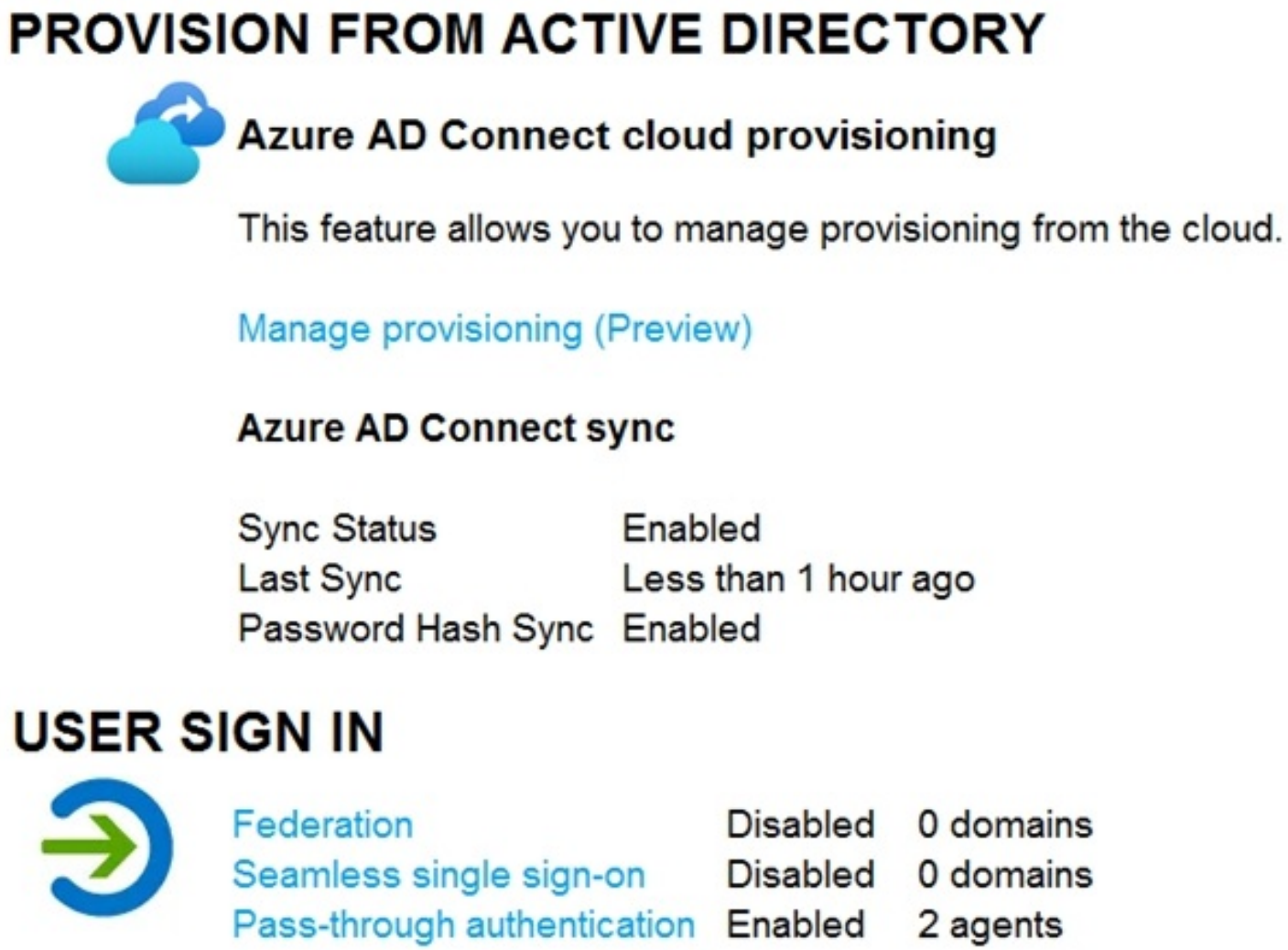
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-change-the-configuration

Question: 16 CertyIQ

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.



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

Answer: A

Explanation:

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.

Reference:

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

Question: 17 CertyIQ

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

Answer: B

Explanation:

Answer is No.

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

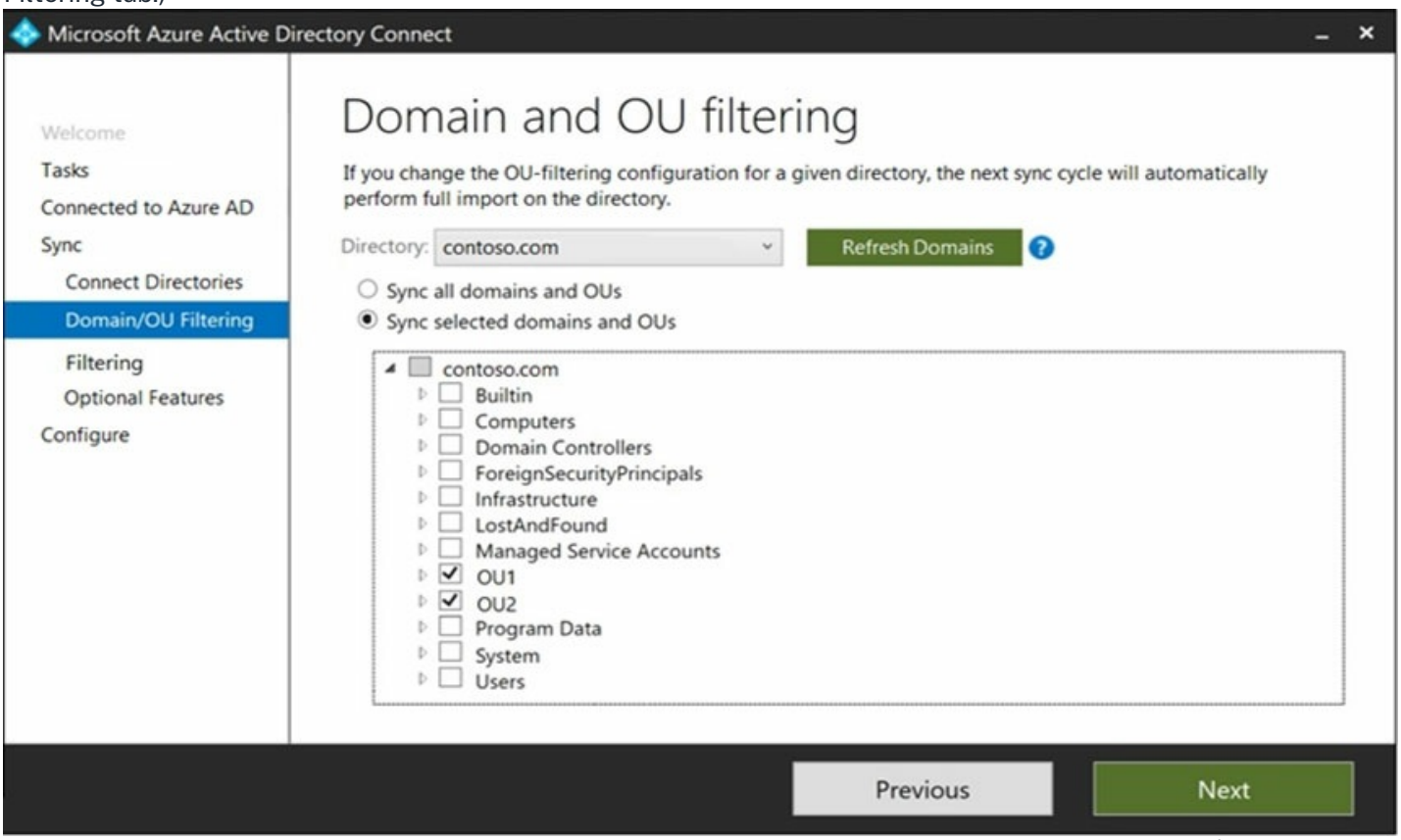
Azure Active Directory (Azure AD) Pass-through Authentication allows your users to sign in to both on-premises and cloud-based applications by using the same passwords. Pass-through Authentication signs users in by validating their passwords directly against on-premises Active Directory.

Question: 18 CertyIQ

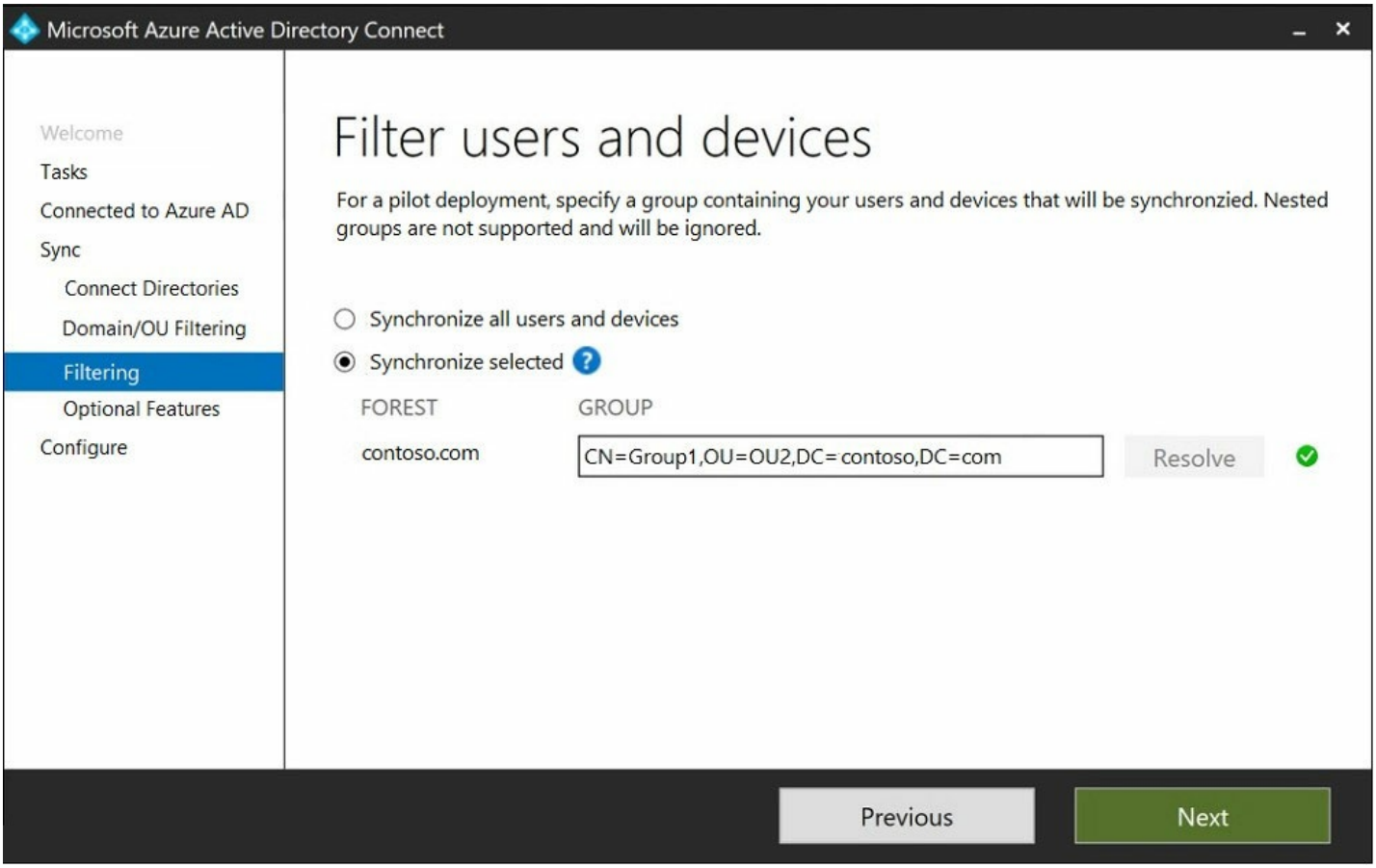
HOTSPOT -
Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the objects shown in the following table.

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.)



For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

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

Answer:

Answer Area

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

Explanation:
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

Question: 19 CertyIQ

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

Answer: C

Explanation:

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

Reference:

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

Question: 20 CertyIQ

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	Answer Area
Delete the contoso.ommicrosoft.com domain.	
Add a custom domain name of contoso.com.	
Set the domain to primary.	
Create a new TXT record in DNS.	
Successfully verify the domain name.	

Answer:

Actions	Answer Area
Delete the contoso.ommicrosoft.com domain.	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.

Explanation:

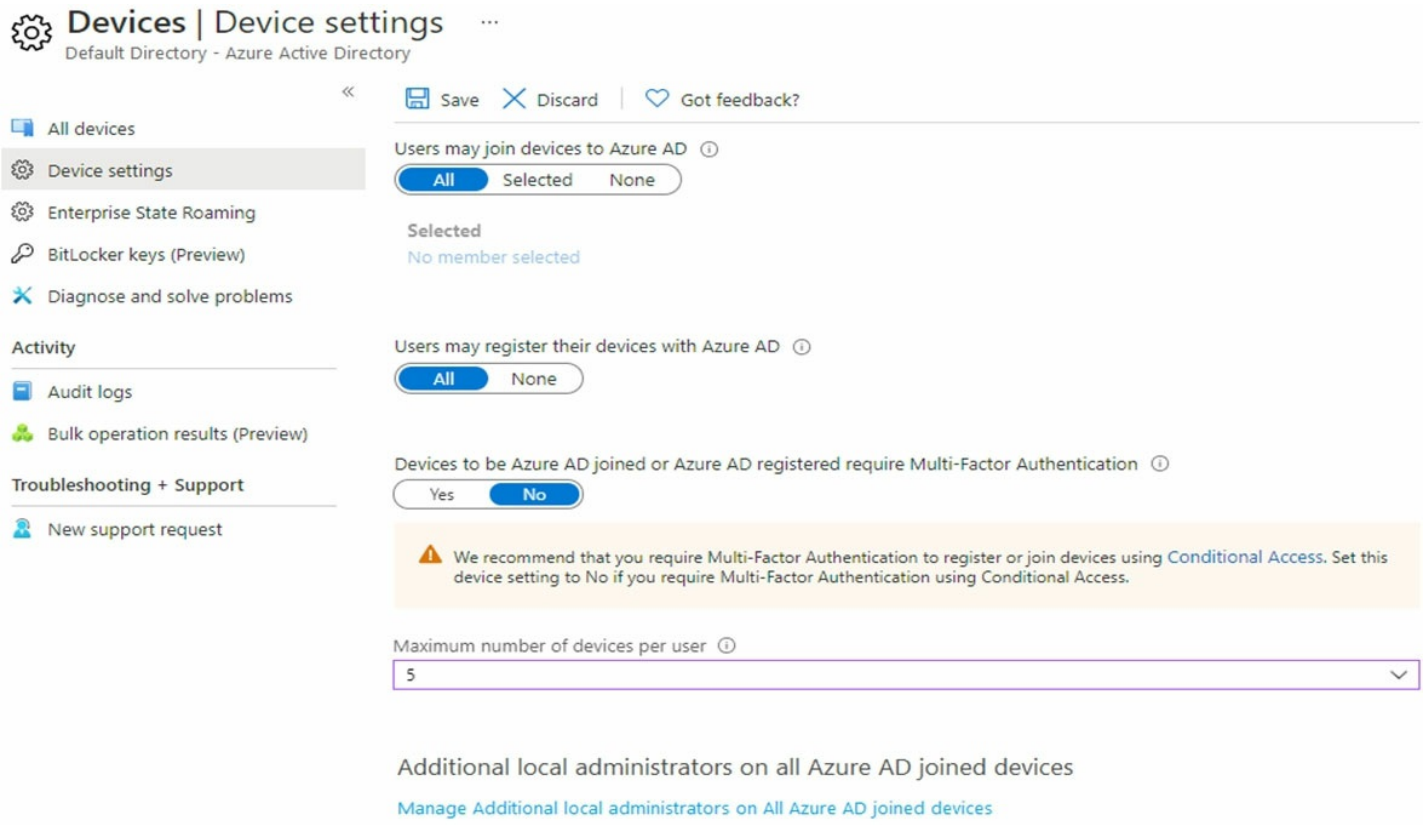
Reference:
https://practical365.com/configure-a-custom-domain-in-office-365/

Question: 21 CertyIQ

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.



User1 has the devices shown in the following table.

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

For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

Statements	Yes	No
User1 can join four additional Windows 10 devices to Azure AD.	○	○
Admin1 can set Devices to be Azure AD joined or Azure AD registered require Multi-Factor Authentication to **Yes**.	○	○
Admin2 is a local administrator on Device3.	○	○

Answer:

Answer Area

Statements	Yes	No
User1 can join four additional Windows 10 devices to Azure AD.	○	○
Admin1 can set Devices to be Azure AD joined or Azure AD registered require Multi-Factor Authentication to **Yes**.	○	○
Admin2 is a local administrator on Device3.	○	○

Explanation:

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

Reference:

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

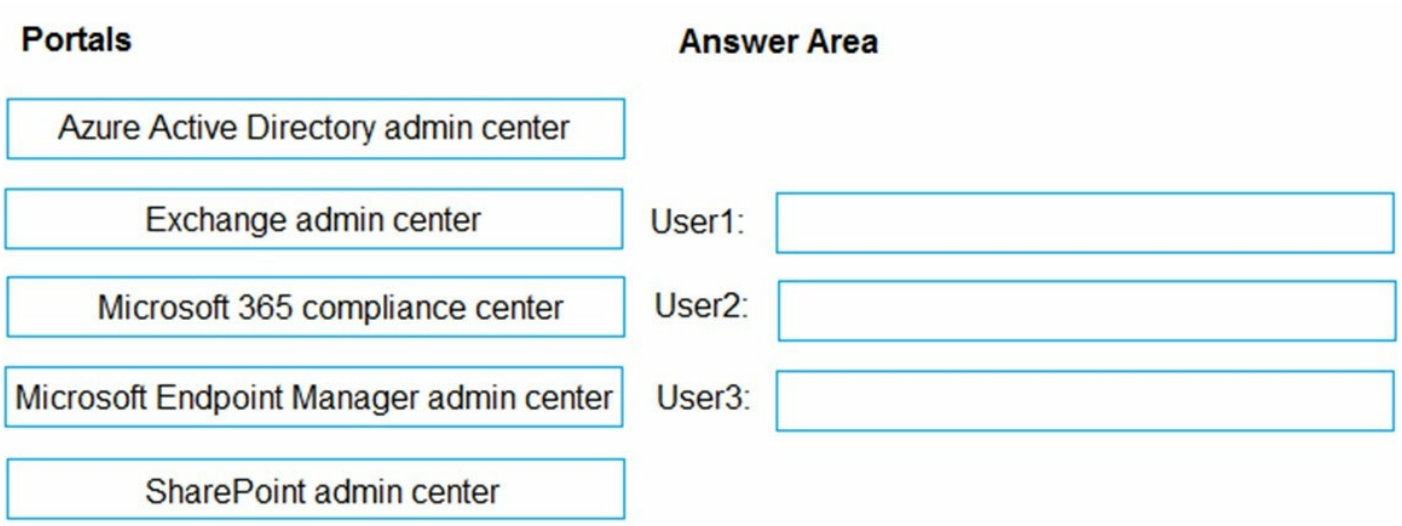
https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal

Question: 22 CertyIQ

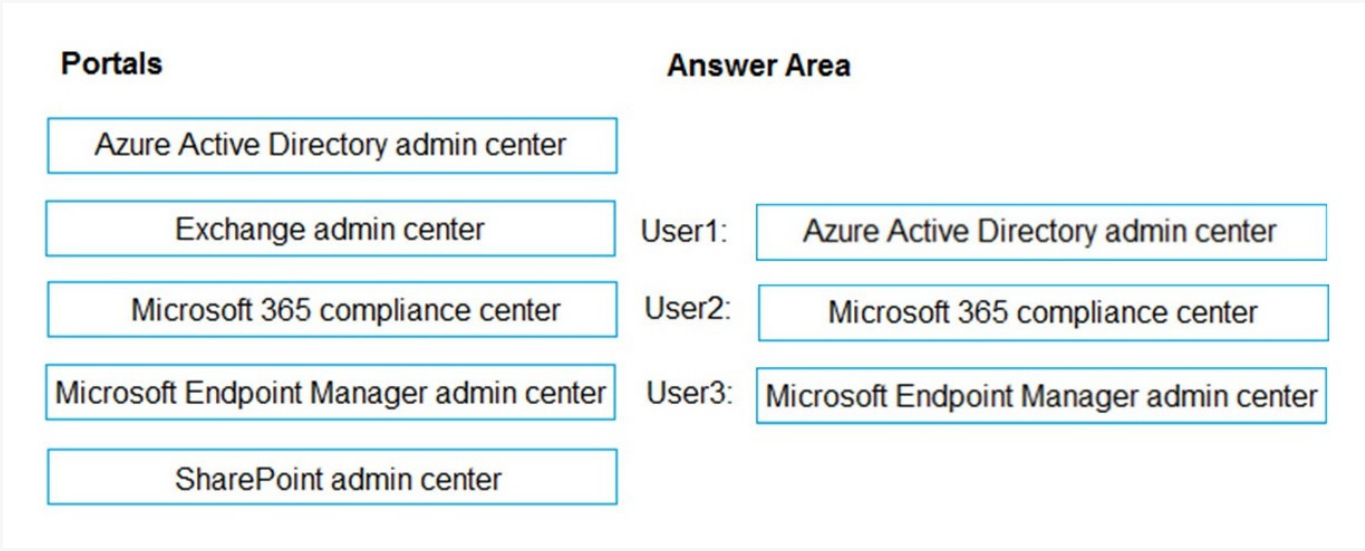
DRAG DROP -
You have a Microsoft 365 E5 subscription that contains three users named User1, User2, and User3.
You need to configure the users as shown in the following table.

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

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



Answer:



Explanation:

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.

Question: 23 CertyIQ

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

Answer: A

Explanation:

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.

Question: 24 CertyIQ

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

Answer: A

Explanation:

In Question, = user1@outlook.com.

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

Question: 25 CertyIQ

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

Answer: D

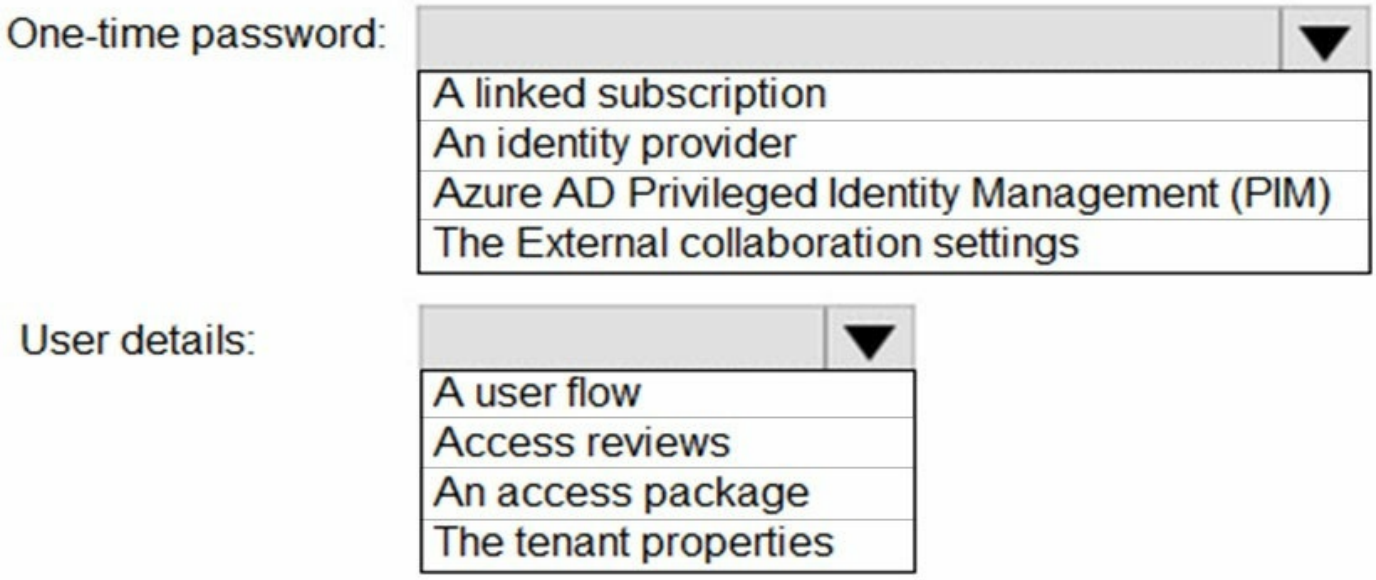
Explanation:
The Set-MsolUserLicense cmdlet updates the license assignment for a user. This can include adding a new license, removing a license, updating the license options, or any combination of these actions.
Note:
There are several versions of this question in the exam. The question has two possible 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

Question: 26 CertyIQ

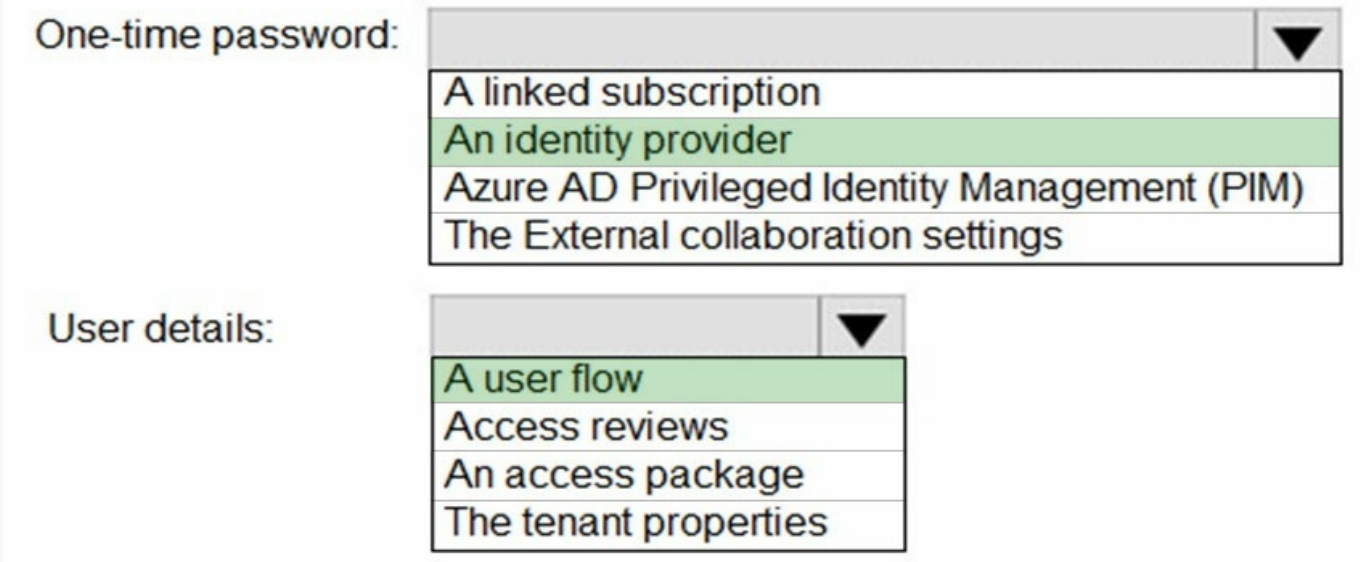
HOTSPOT -
You have an Azure Active Directory (Azure AD) tenant and an Azure web app named App1.
You need to provide guest users with self-service sign-up for App1. The solution must meet the following requirements:
- Guest users must be able to sign up by using a one-time password.
- The users must provide 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



Answer:

Answer Area



Explanation:

- 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.

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

Question: 27 CertyIQ

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

Answer: C

Explanation:

Name [displayName] -> Required

User name [userPrincipalName] -> Required

Initial password [passwordProfile] -> Required,

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

Reference:

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

Question: 28 CertyIQ

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.

Answer: C

Explanation:

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:

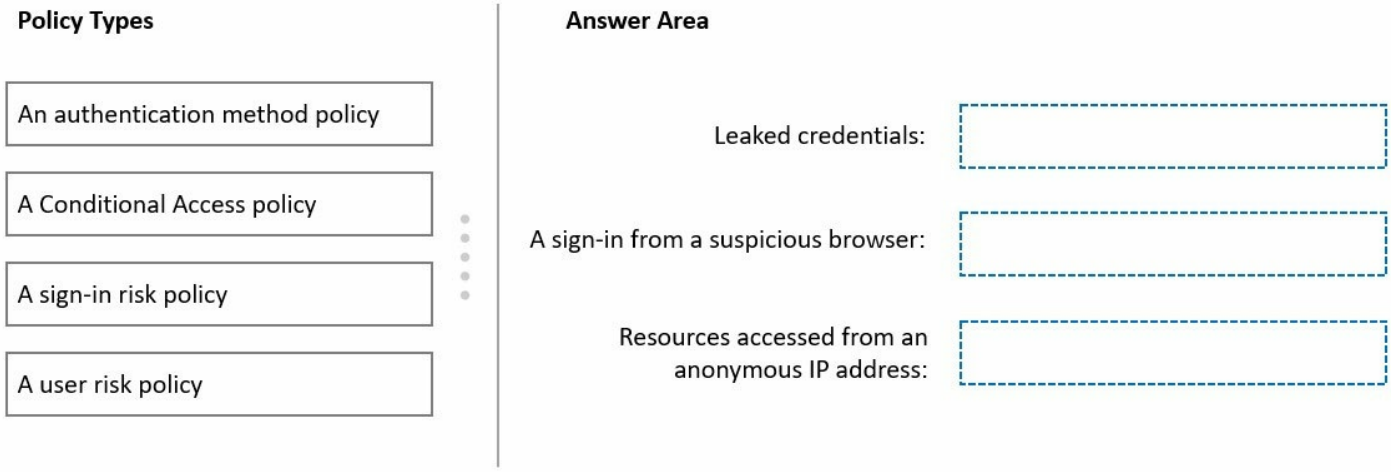
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso-quick-start

Reference:

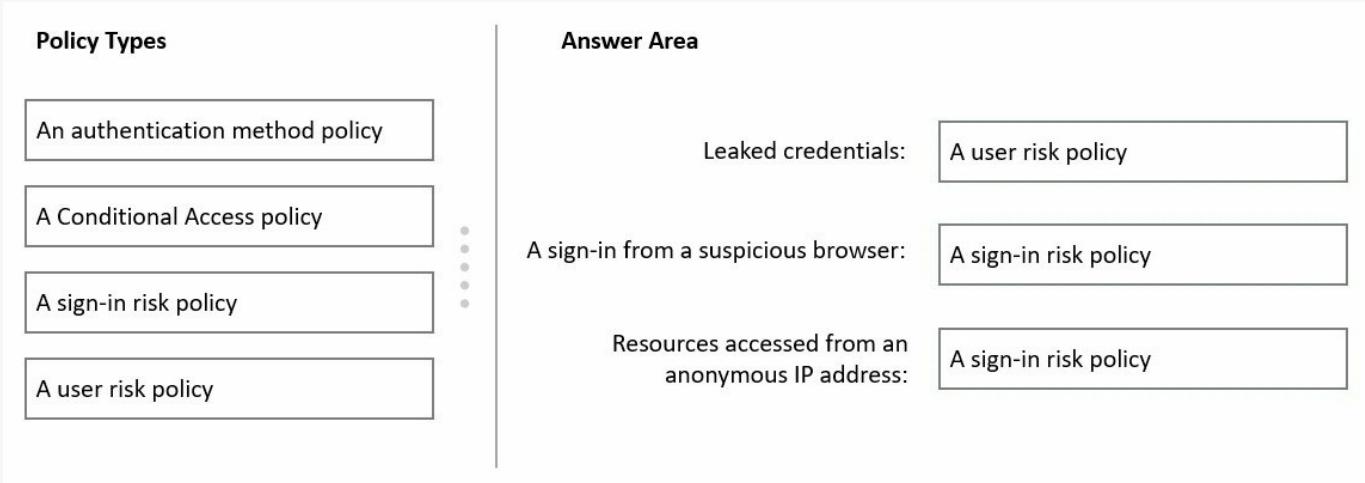
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso-quick-start

Question: 29 CertyIQ

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:



Answer:



Explanation:

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.

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

Reference:

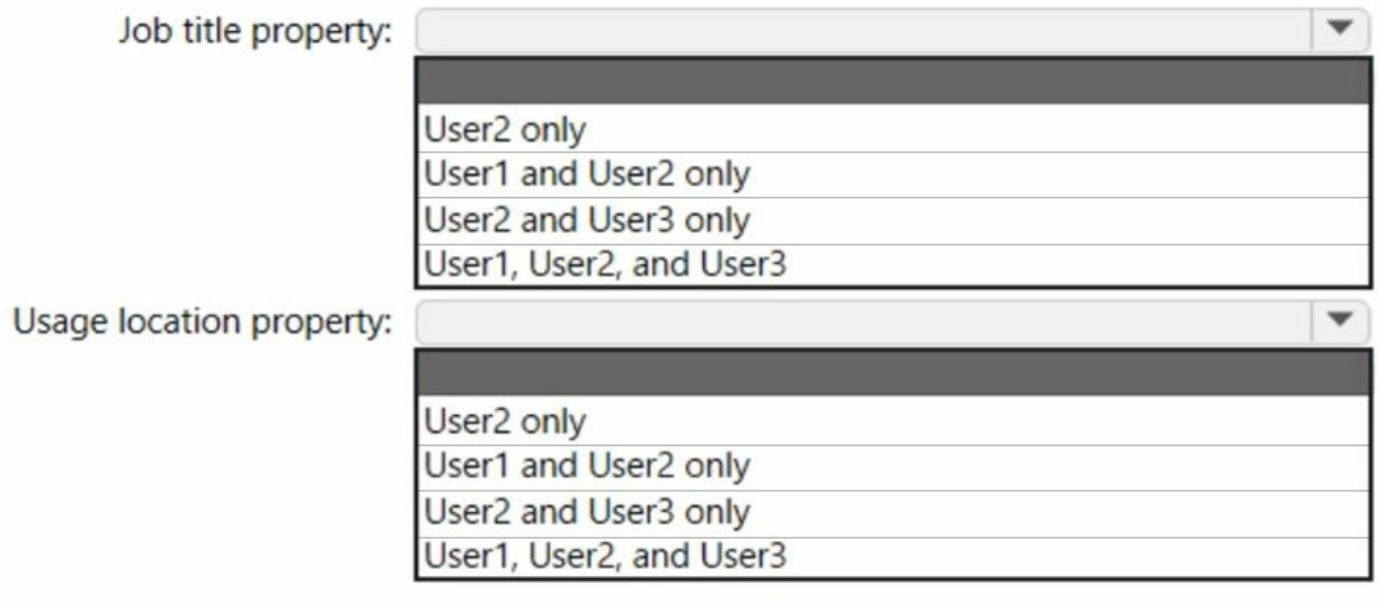
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies

Question: 30 CertyIQ

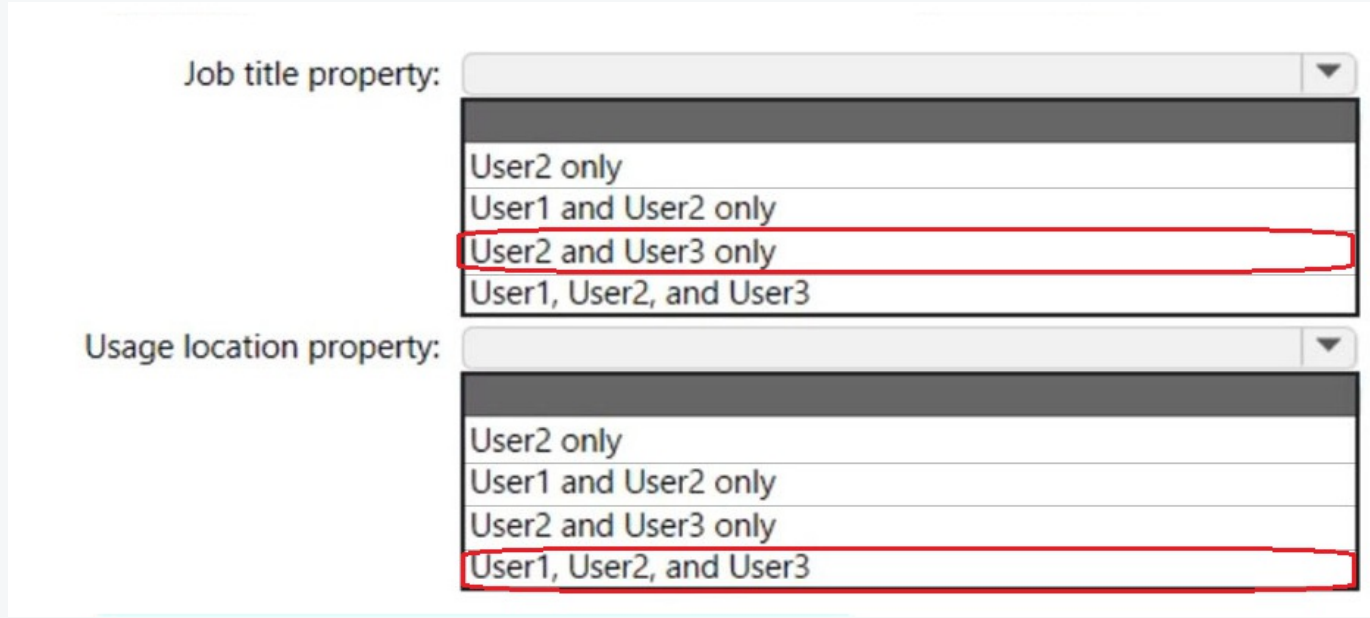
HOTSPOT -
You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

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:



Answer:



Explanation:

Box 1: User2 and User3 only

See

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

It states: Note

“You must use Windows Server Active Directory to update the identity, contact info, or job info for users whose source of authority is Windows Server Active Directory. After you complete your update, you must wait for the next synchronization cycle to complete before you'll see the changes.”

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

Question: 31 CertyIQ

You have an Azure Active Directory (Azure AD) tenant that: contains a user named User1.
You need to ensure that User1 can create new catalogs and add1 resources to the catalogs they own.
What should you do?

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

Answer: C

Explanation:
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

Question: 32 CertyIQ

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.

Answer: C

Explanation:

The question states: You need to configure the Windows 10 computers to support Azure AD Seamless SSO.

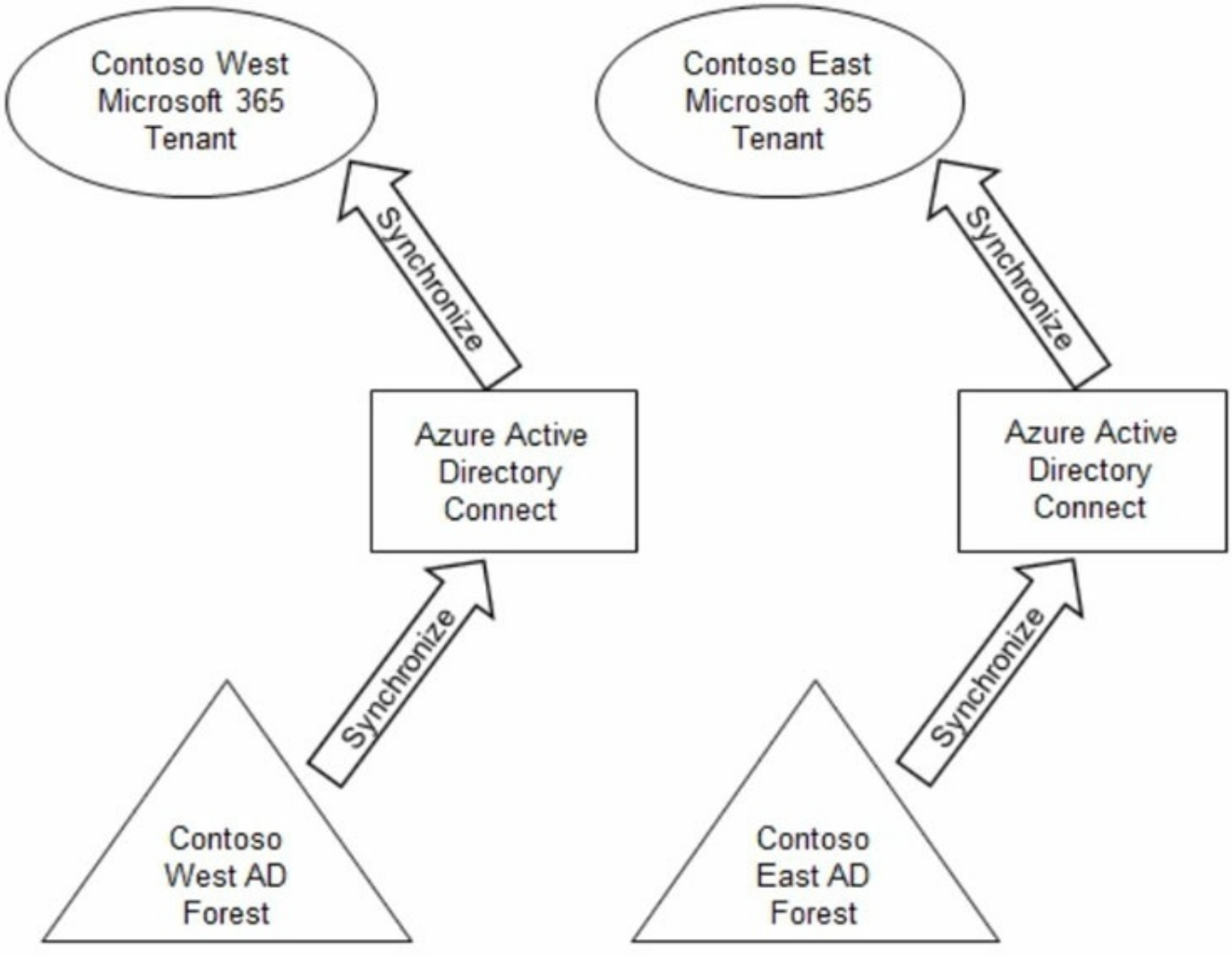
The catch is, "configure the Windows 10 computers.

The answer is C.

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

Question: 33 CertyIQ

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.

Answer: B

Explanation:
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

Question: 34 CertyIQ

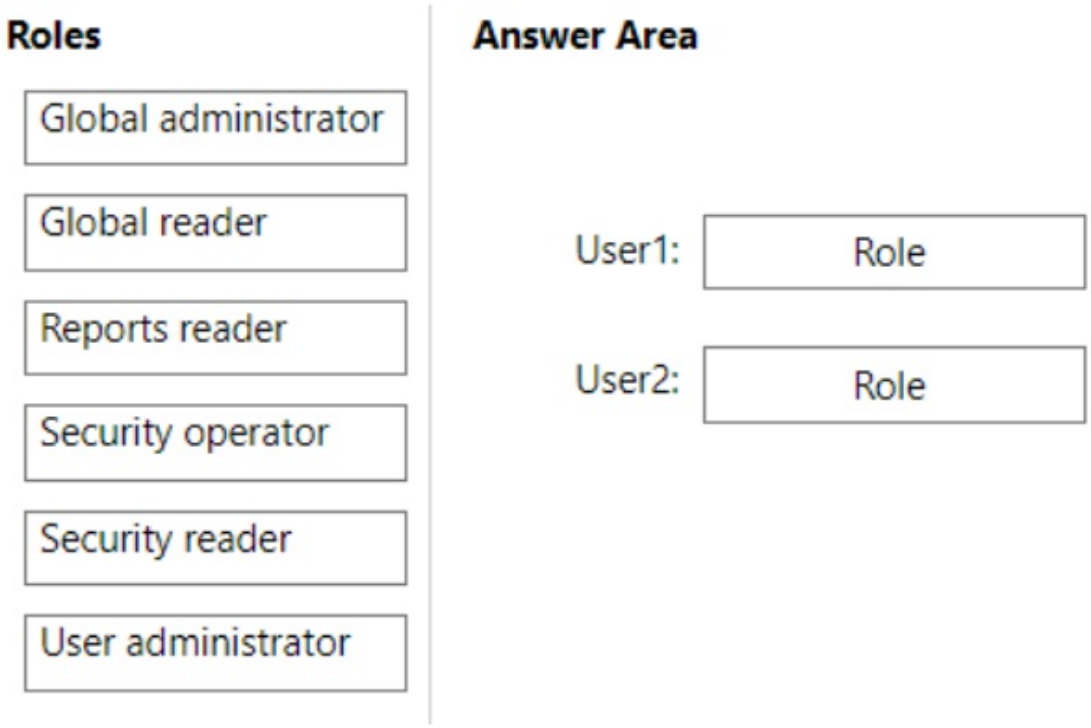
DRAG DROP
-

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

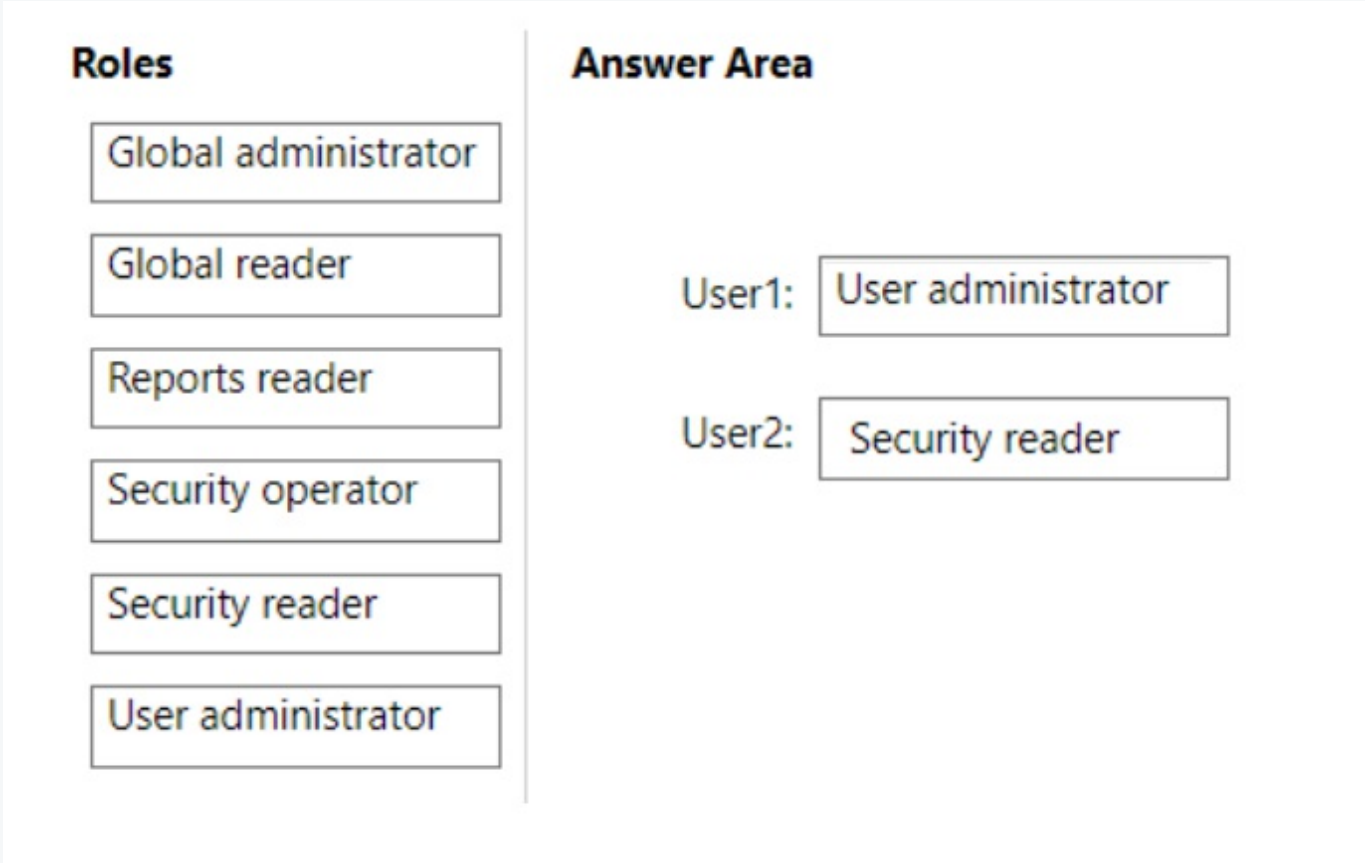
You need to ensure that User1 can create access reviews for groups, and that User2 can review the history report for all the completed access reviews. The solution must use the principle of least privilege.

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.



Answer:



Explanation:

User Administrator

Security Reader

Reference:

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

Question: 35 CertyIQ

HOTSPOT
-

You have an Azure subscription.

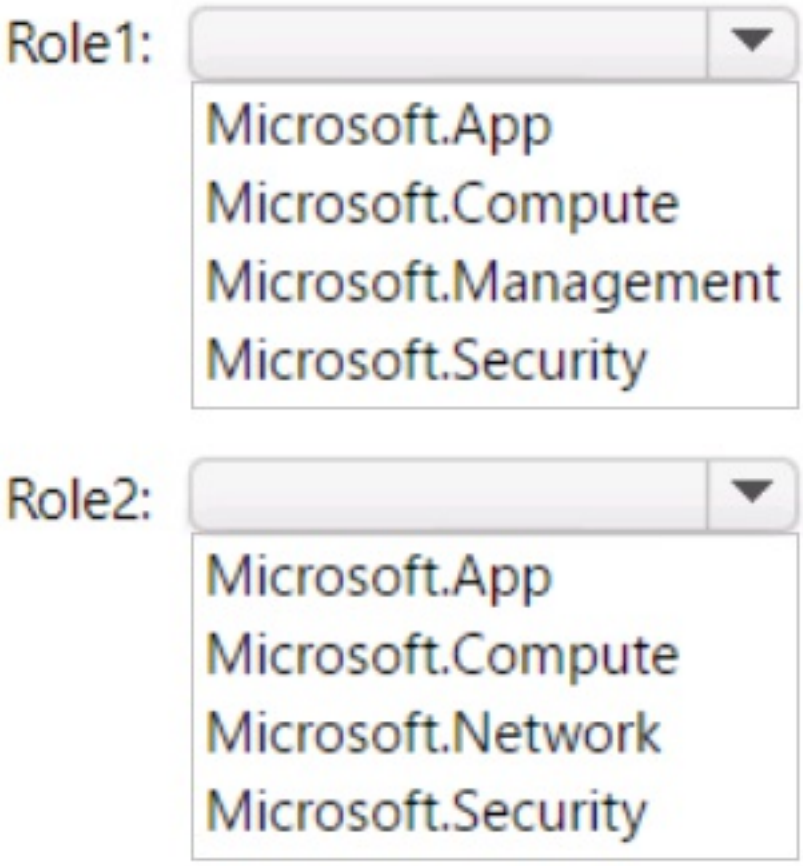
You need to create two custom roles named Role1 and Role2. The solution must meet the following requirements:

• 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.

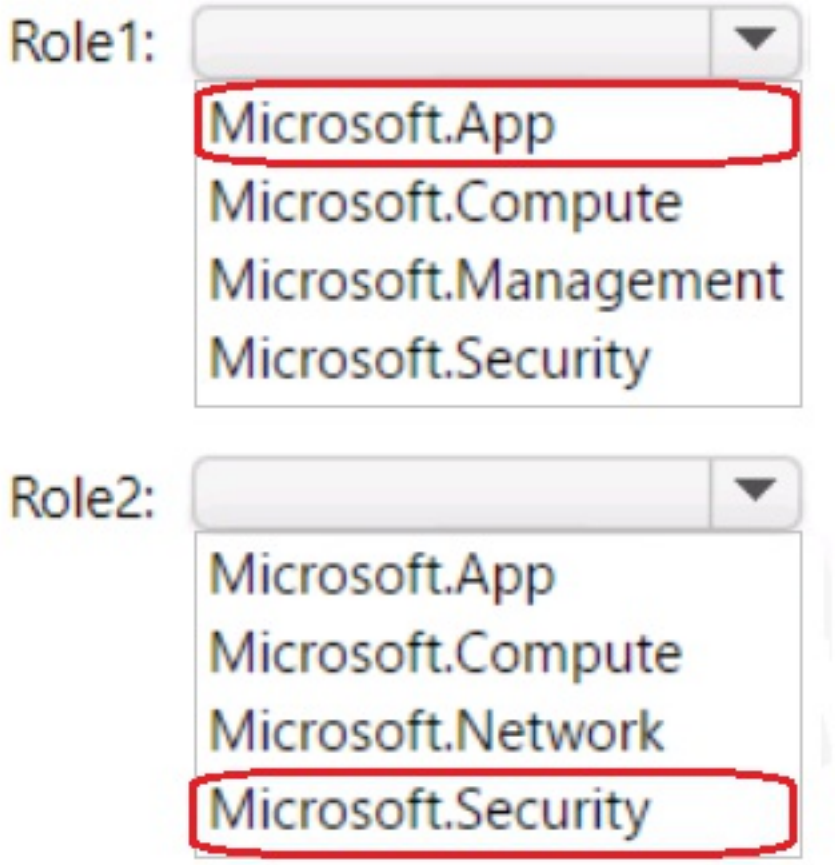
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area



Explanation:

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)

Question: 36 CertyIQ

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.

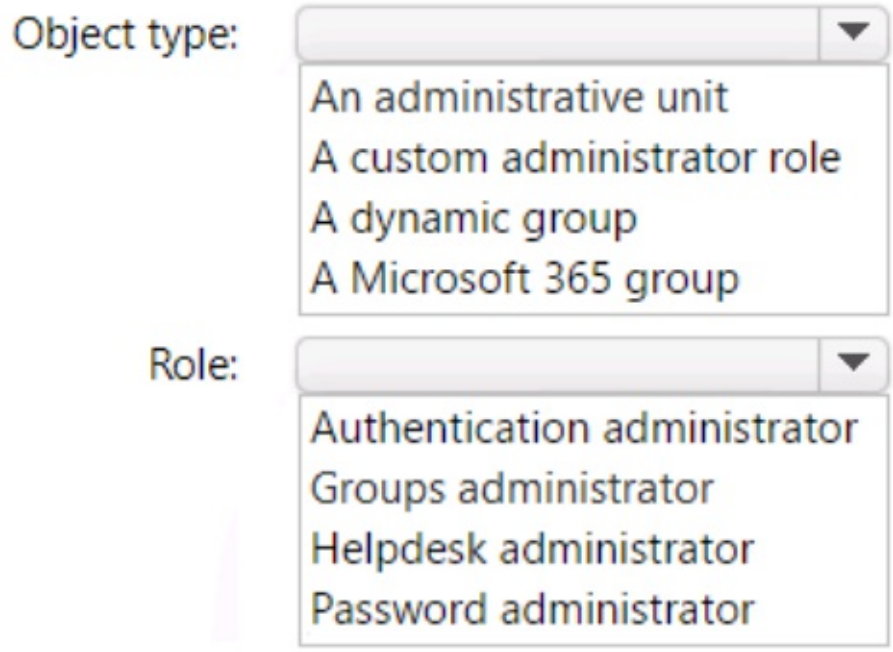
You need to ensure that the support team can reset passwords and manage multi-factor authentication (MFA)

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



Answer:

Answer Area

Explanation:

Object Type: Administrative Unit

Role: Authentication administrator

Question: 37 CertyIQ

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

Answer: D

Explanation:

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

Question: 38 CertyIQ

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

Answer: D

Explanation:

According to operators precedence we can consider the following parenthesis: (statement1 -and statement2 -and statement3) -or (statement4). So, the results is the sub-result of the first parenthesis plus the results of the second one. So, it's D.

Question: 39 CertyIQ

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

Answer: D

Explanation:

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

Question: 40 CertyIQ

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

Answer: A

Explanation:

A. el cmdlet Set-MsolUserLicense

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.

Question: 41 CertyIQ

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

Answer: D

Explanation:

Correct answer is D: the Set-MsolUserLicense cmdlet.

Question: 42 CertyIQ

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:

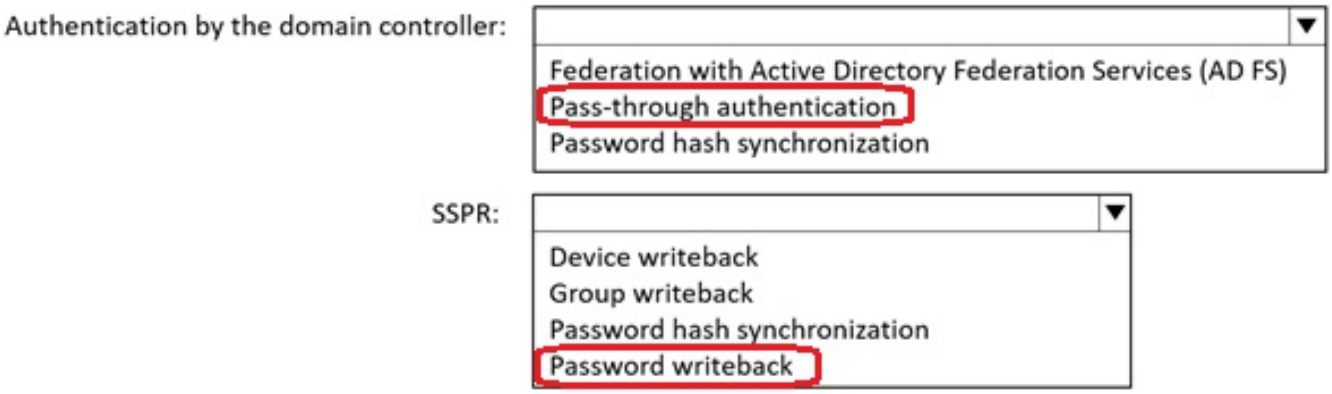
- Federation with Active Directory Federation Services (AD FS)
- Pass-through authentication
- Password hash synchronization

SSPR:

- Device writeback
- Group writeback
- Password hash synchronization
- Password writeback

Answer:

Answer Area



Explanation:

pass- through auth

password write back

Question: 43 CertyIQ

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

Answer: D

Explanation:

the Set-MsolUserLicense cmdlet.

Question: 44 CertyIQ

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

Answer: B

Explanation:

No is a correct answer.

Question: 45 CertyIQ

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

Answer: A

Explanation:

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

Question: 46 CertyIQ

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

Answer: B

Explanation:

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

Question: 47 CertyIQ

HOTSPOT
-

Case Study
-

Overview
-

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

Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.

Existing Environment. Existing Environment

The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named Contoso_Resources. The Contoso_Resources OU contains all users and computers.

The contoso.com Active Directory domain contains the relevant users shown in the following table.

Name	Office	Department
Admin1	Montreal	Helpdesk
User1	Montreal	HR
User2	Montreal	HR
User3	Montreal	HR
Admin2	London	Helpdesk
User4	London	Finance
User5	London	Sales
User6	London	Sales
Admin3	Seattle	Helpdesk
User7	Seattle	Sales
User8	Seattle	Sales
User9	Seattle	Sales

Contoso also includes a marketing department that has users in each office.

Existing Environment. Microsoft 365/Azure Environment

Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:

•Microsoft Office 365 Enterprise E5
•Enterprise Mobility + Security E5
•Windows 10 Enterprise E3
•Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso_Resources OU is synced.

Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.

User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:

•The users in the London office have the Microsoft 365 Phone System license unassigned.
•The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

Existing Environment. Problem Statements

Contoso identifies the following issues:

•Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.
•The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.
•The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.
•Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.
•When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes
-

Contoso plans to implement the following changes:

•Implement self-service password reset (SSPR).
•Analyze Azure audit activity logs by using Azure Monitor.
•Simplify license allocation for new users added to the tenant.
•Collaborate with the users at Fabrikam on a joint marketing campaign.
•Configure the User administrator role to require justification and approval to activate.
•Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.
•For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

Contoso plans to acquire a company named ADatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.

Requirements. Technical Requirements

Contoso identifies the following technical requirements:

•All users must be synced from AD DS to the contoso.com Azure AD tenant.
•App1 must have a redirect URI pointed to https://contoso.com/auth-response.
•License allocation for new users must be assigned automatically based on the location of the user.
•Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.
•Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.
•The helpdesk administrators must be able to manage licenses for only the users in their respective office.
•Users must be forced to change their password if there is a probability that the users' identity was compromised.

You need to meet the technical requirements for license management by the help desk administrators.

What should you create first, and which tool should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Object to create for each branch office:

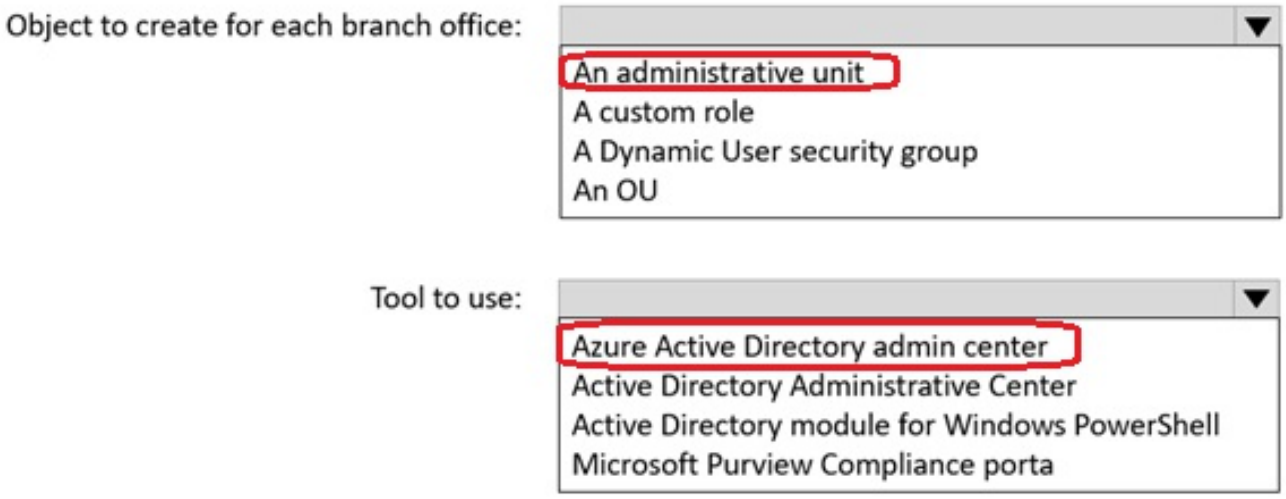
- An administrative unit
- A custom role
- A Dynamic User security group
- An OU

Tool to use:

- Azure Active Directory admin center
- Active Directory Administrative Center
- Active Directory module for Windows PowerShell
- Microsoft Purview Compliance porta

Answer:

Answer Area



Explanation:

An administrative unit.

Azure Active Directory Admin center.

Question: 48

CertyIQ

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

Answer: A

Explanation:

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.

Question: 49 CertyIQ

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.

Answer: B

Explanation:

Recreate the IT_Group1 group.

Question: 50 CertyIQ

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

Answer: B

Explanation:

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

Question: 51 CertyIQ

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

Answer: A

Explanation:

Answer is A. A group cannot be added as a member of role assignable group. You cannot add a Dynamic user membership type.

https://learn.microsoft.com/en-us/azure/active-directory/roles/groups-concept

Question: 52 CertyIQ

HOTSPOT
-

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

You need to configure External collaboration settings for the tenant to meet the following requirements:

•Guest users must be prevented from querying staff email addresses.
•Guest users must be able to access the tenant only if they are invited by User1.

Which three settings should you configure? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Guest user access restrictions:

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

Guest invite restrictions:

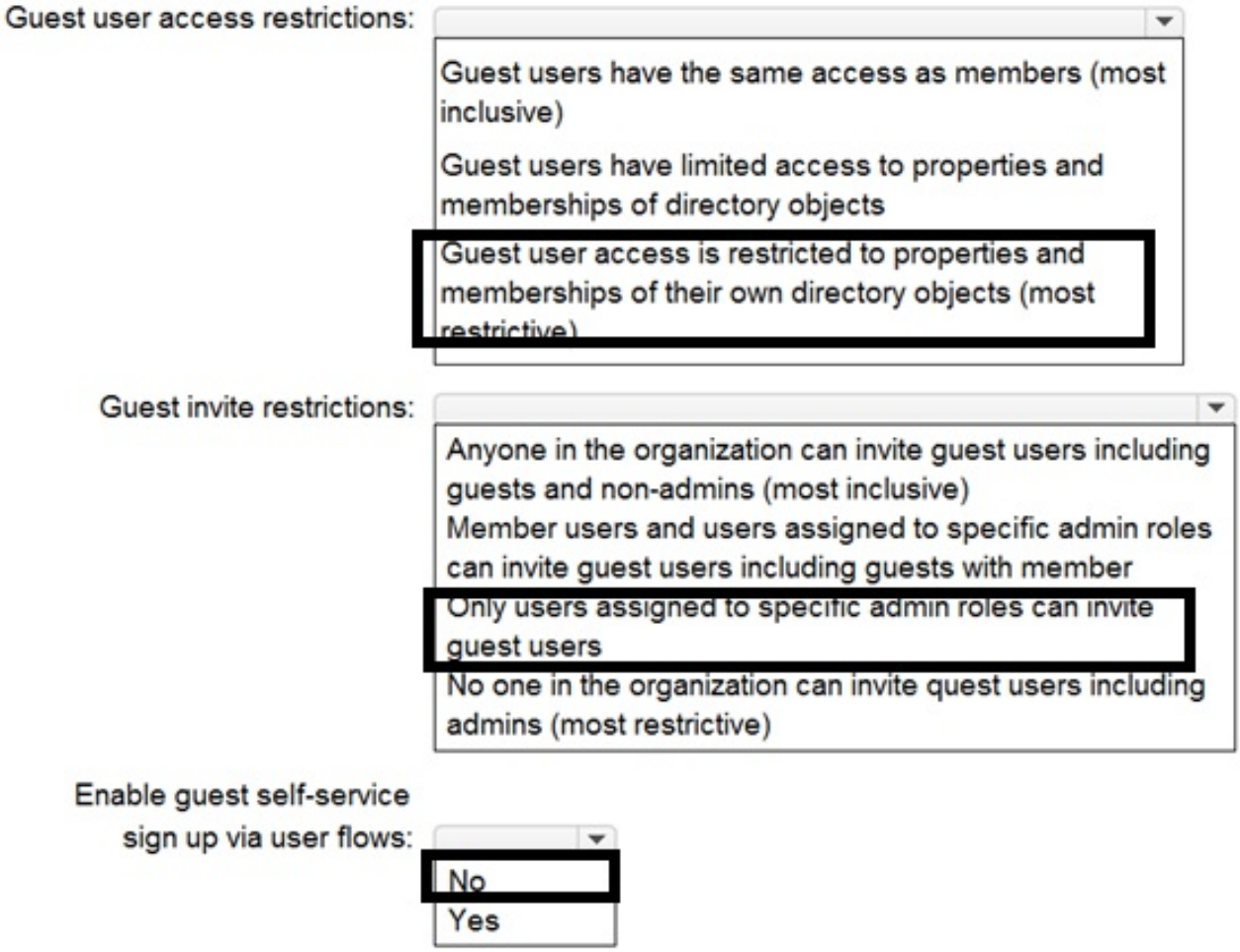
- Anyone in the organization can invite guest users including guests and non-admins (most inclusive)
- Member users and users assigned to specific admin roles can invite guest users including guests with member
- Only users assigned to specific admin roles can invite guest users
- No one in the organization can invite quest users including admins (most restrictive)

Enable guest self-service sign up via user flows:

- No
- Yes

Answer:

Answer Area



Question: 53 CertyIQ

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

Answer: D

Explanation:

The Licenses blade in the Azure Active Directory admin center.

Question: 54 CertyIQ

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

Answer: B

Explanation:

B With read and write access, you can make changes and directly interact with identity secure score.Global administratorSecurity administrator Exchange administrator SharePoint administratorSecurity 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

Question: 55 CertyIQ

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

Answer: A

Explanation:

From Microsoft:With read and write access, you can make changes and directly interact with identity secure score.Global administratorSecurity administratorExchange administratorSharePoint administrator

https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/identity-secure-score#who-can-use-the-identity-secure-score

Question: 56 CertyIQ

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.

Answer: C

Explanation:

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

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

Question: 57 CertyIQ

HOTSPOT
-

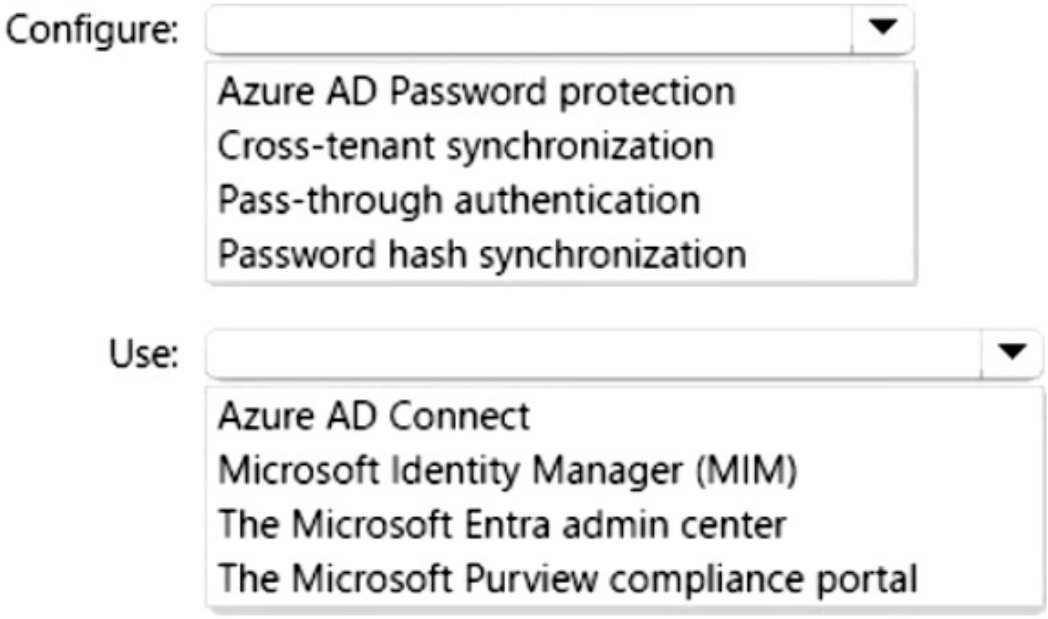
Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with an Azure AD tenant.

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.

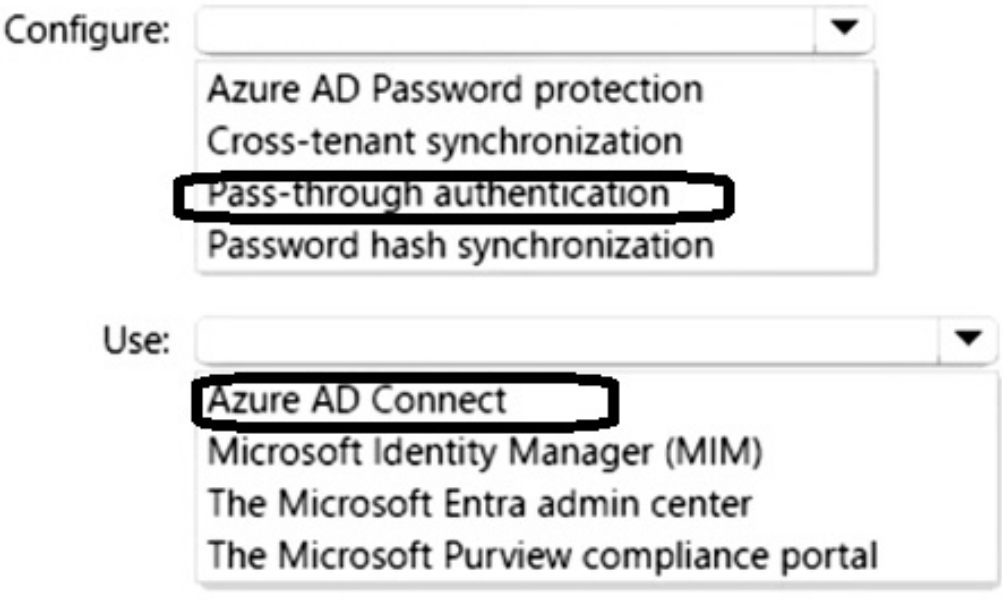
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area

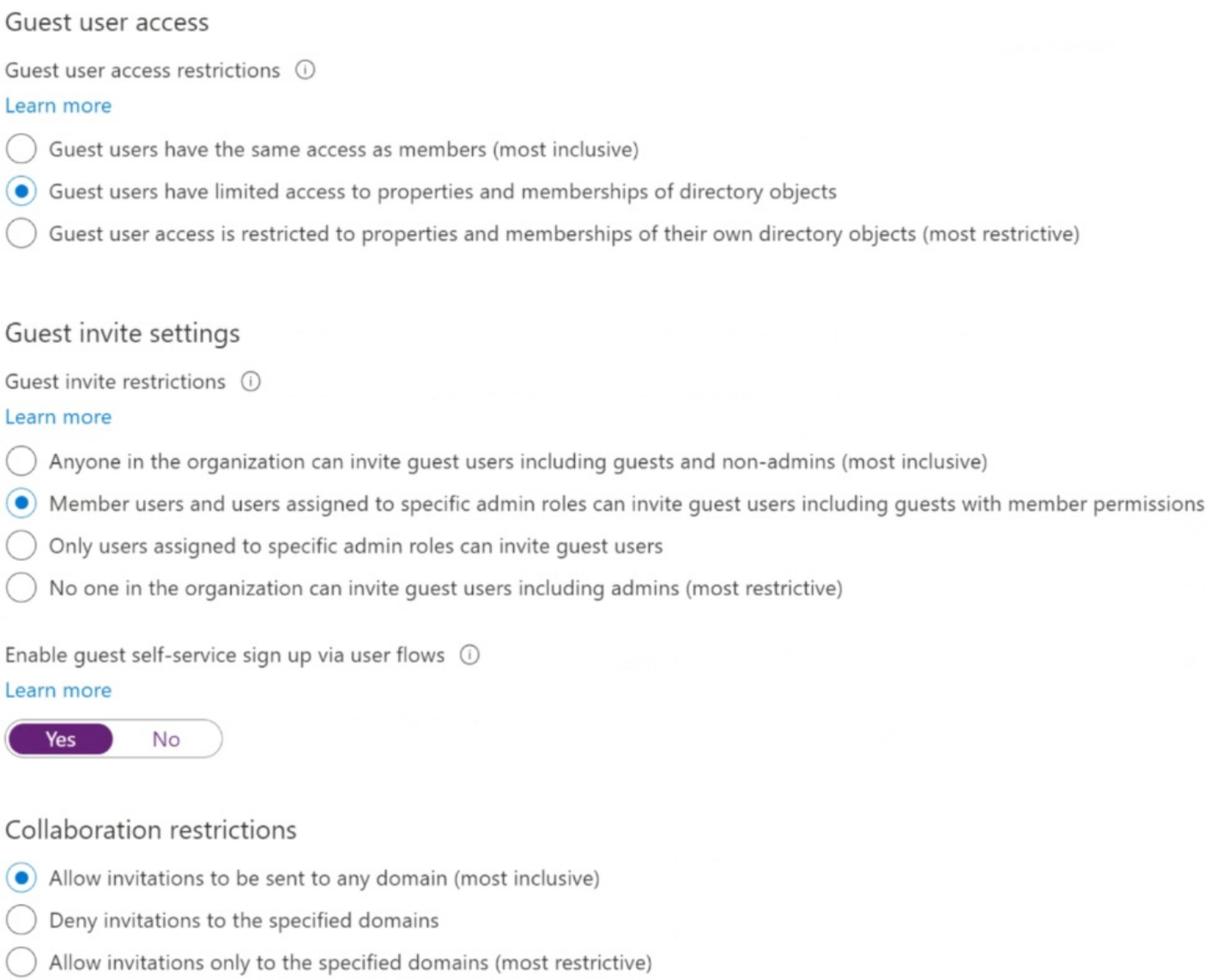


Explanation:

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

Question: 58 CertyIQ

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.)



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

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

Which users will be emailed a passcode?

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

Answer: A

Explanation:

In Question, = bsmith@fabrikam.com

Correct Answer = A

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

Question: 59 CertyIQ

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

Answer: B

Explanation:

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.

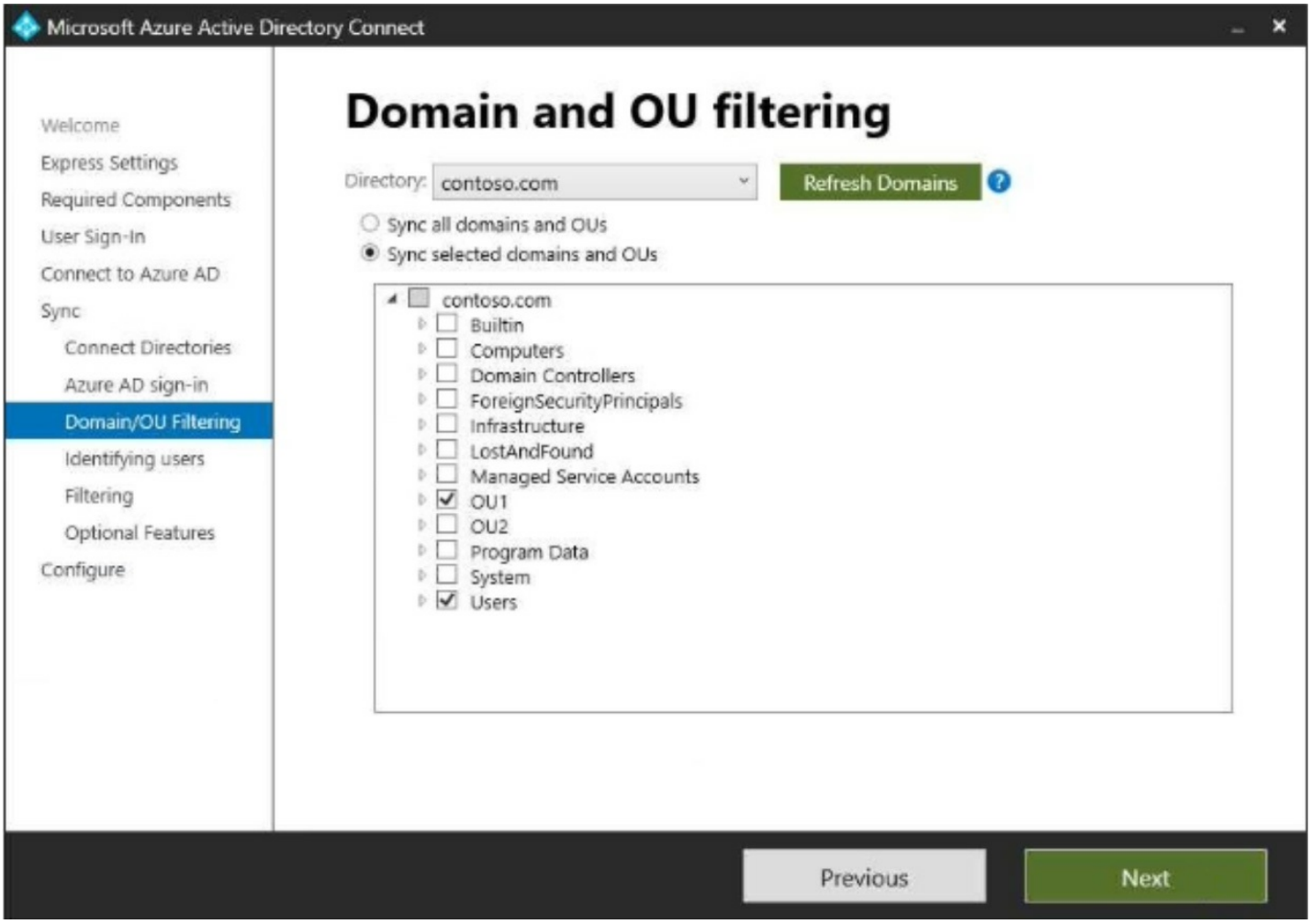
Question: 60 CertyIQ

HOTSPOT
-

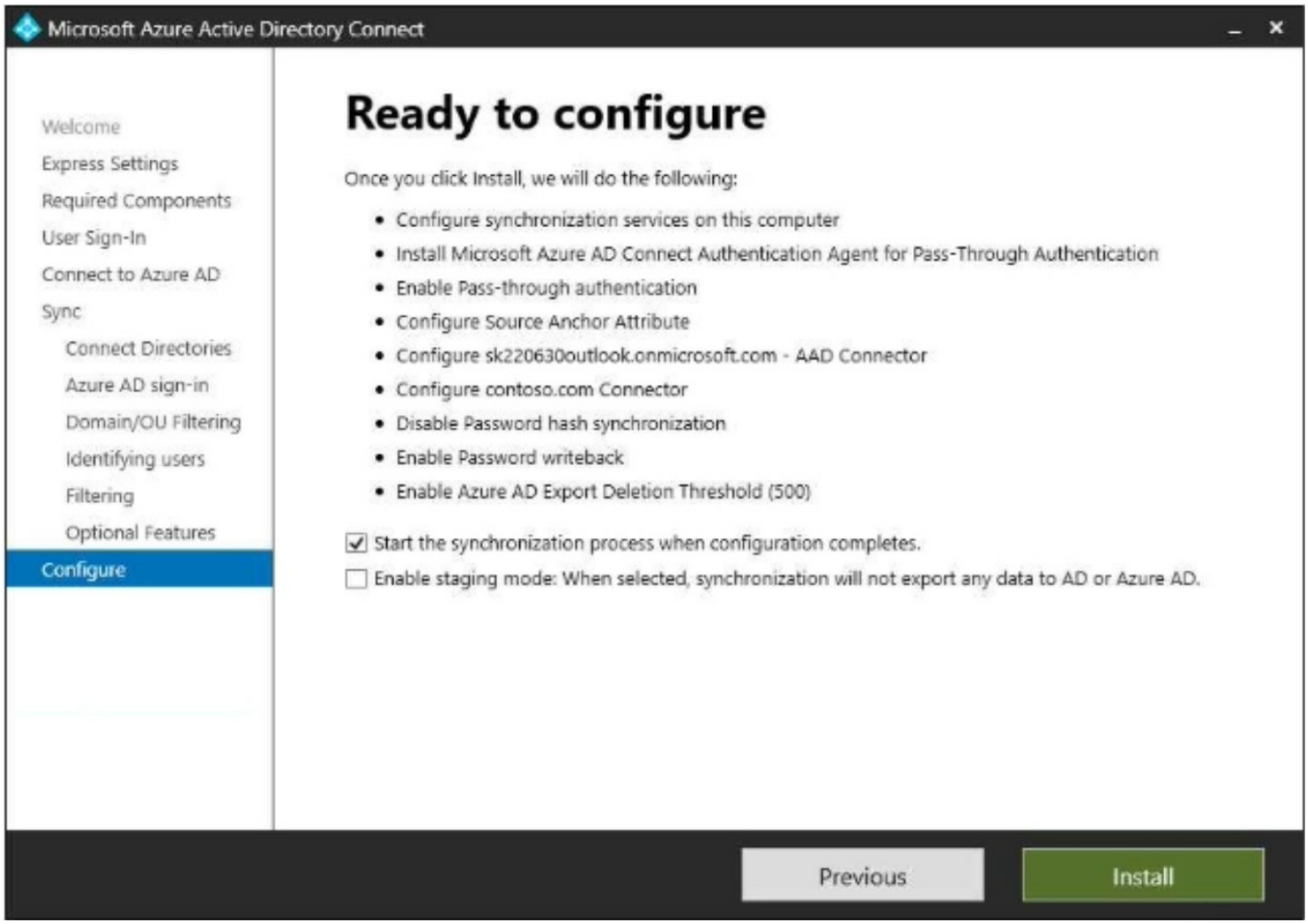
Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with Azure AD and contains the users shown in the following table.

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.	○	○
If User1 accesses Microsoft Exchange Online, he will be authenticated by an on-premises domain controller.	○	○
User2 can be added to a Microsoft SharePoint Online site as a member.	○	○

Answer:

Answer Area

Statements	Yes	No
User1 can use self-service password reset (SSPR) to reset his password.	○	○
If User1 accesses Microsoft Exchange Online, he will be authenticated by an on-premises domain controller.	○	○
User2 can be added to a Microsoft SharePoint Online site as a member.	○	○

Explanation:

yes

yes

No

Question: 61 CertyIQ

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

Answer: B

Explanation:

the Licenses blade in the Azure Active Directory admin center

Question: 62 CertyIQ

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

Answer: B

Explanation:

Correct answer is B:the Microsoft 365 admin center.

Reference:

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

Question: 63 CertyIQ

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

Answer: B

Explanation:

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.

Question: 64

CertyIQ

HOTSPOT
-

You have an Azure AD tenant.

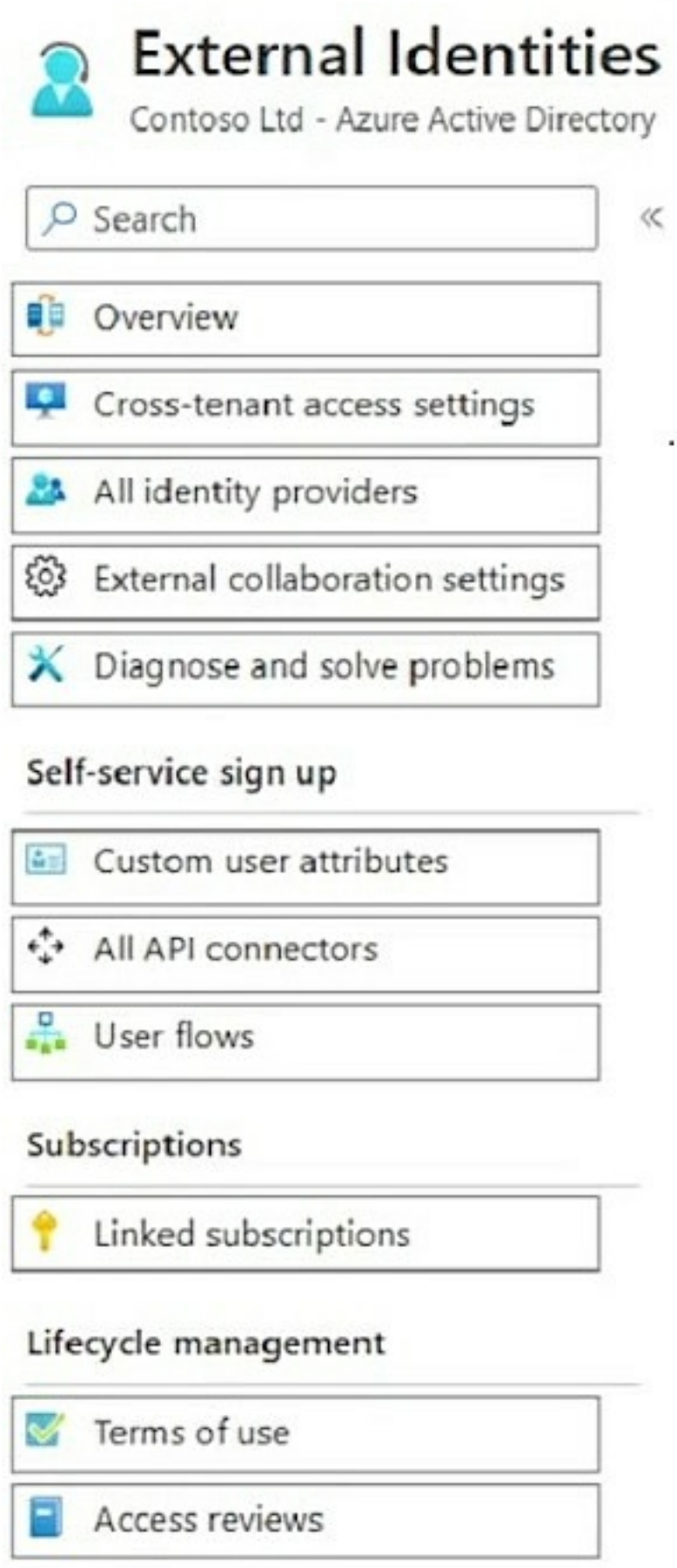
You need to configure the following External Identities features:

•B2B collaboration
•Monthly active users (MAU)-based pricing

Which two settings should you configure? To answer, select the settings in the answer area.

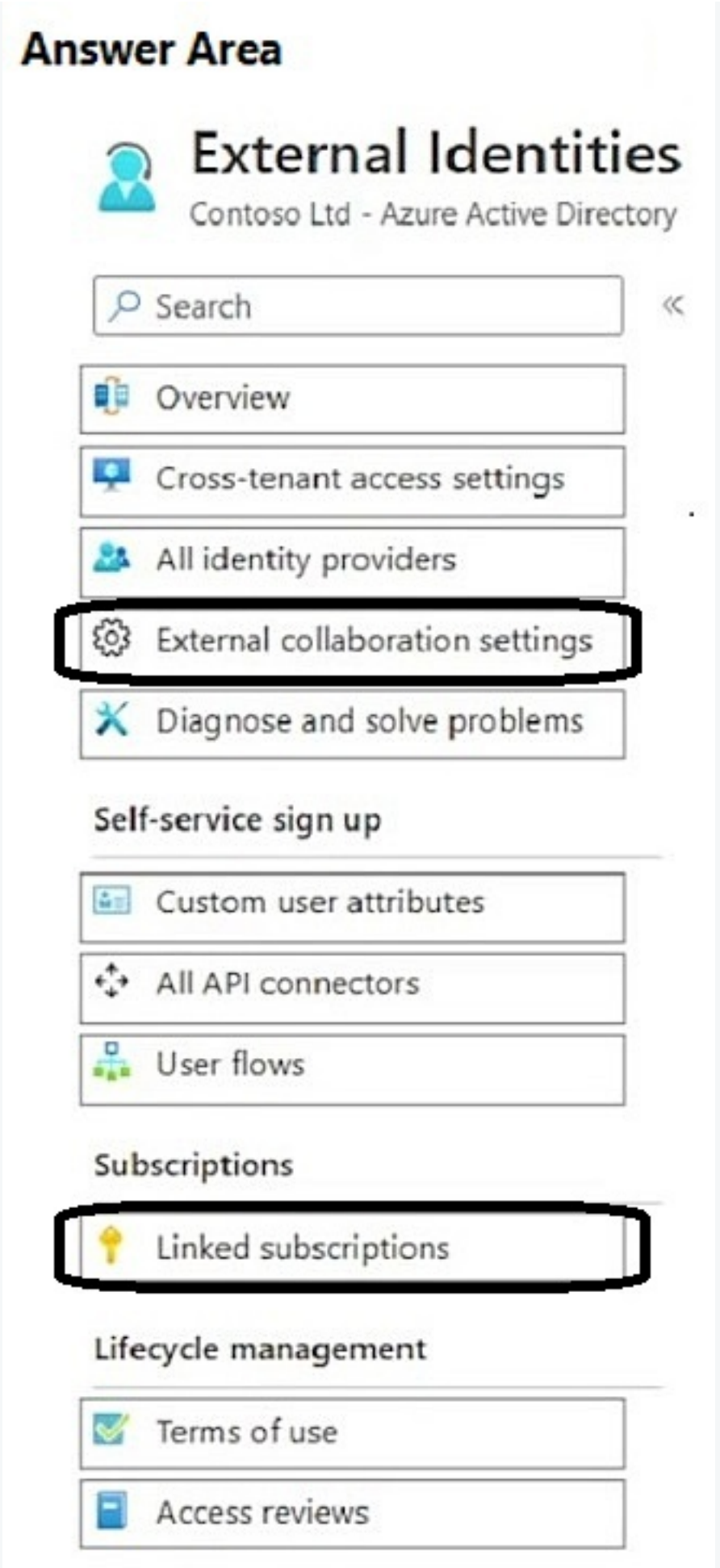
NOTE: Each correct selection is worth one point.

Answer Area

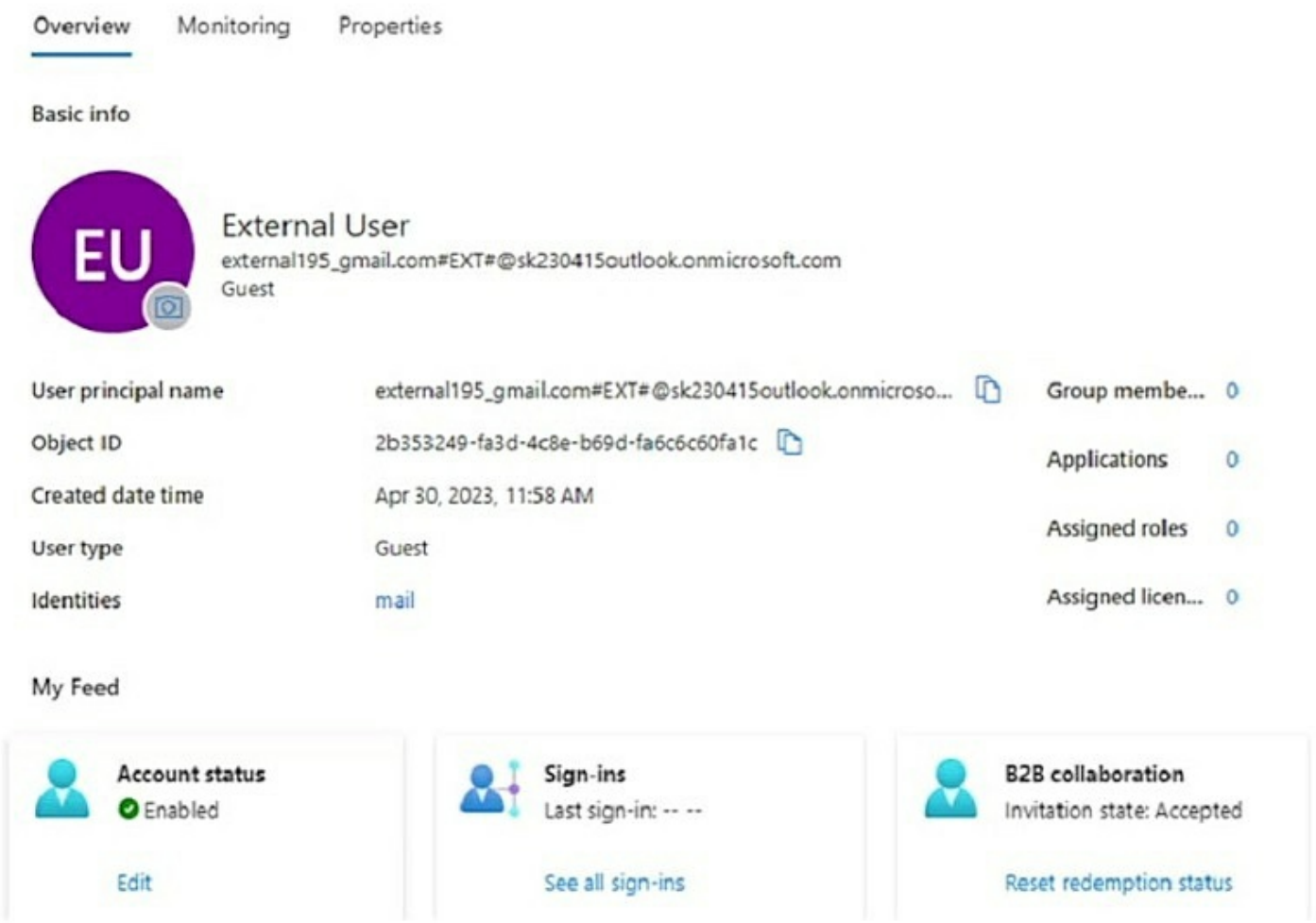


Answer:

Answer Area


External Identities
Contoso Ltd - Azure Active Directory
Search
Overview
Cross-tenant access settings
All identity providers
External collaboration settings
Diagnose and solve problems
Self-service sign up
Custom user attributes
All API connectors
User flows
Subscriptions
Linked subscriptions
Lifecycle management
Terms of use
Access reviews

You have an Azure AD tenant that contains the external user shown in the following exhibit.



You update the email address of the user.

You need to ensure that the user can authenticate by using the updated email address.

What should you do for the user?

A.Modify the Authentication methods settings.
B.Reset the password.
C.Revoke the active sessions.
D.Reset the redemption status.

Answer: D

Explanation:

https://learn.microsoft.com/en-us/entra/external-id/reset-redemption-statusupdate 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•etcTo 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.

Question: 66 CertyIQ

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

Answer: A

Explanation:

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.

Question: 67 CertyIQ

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.

Answer: B

Explanation:

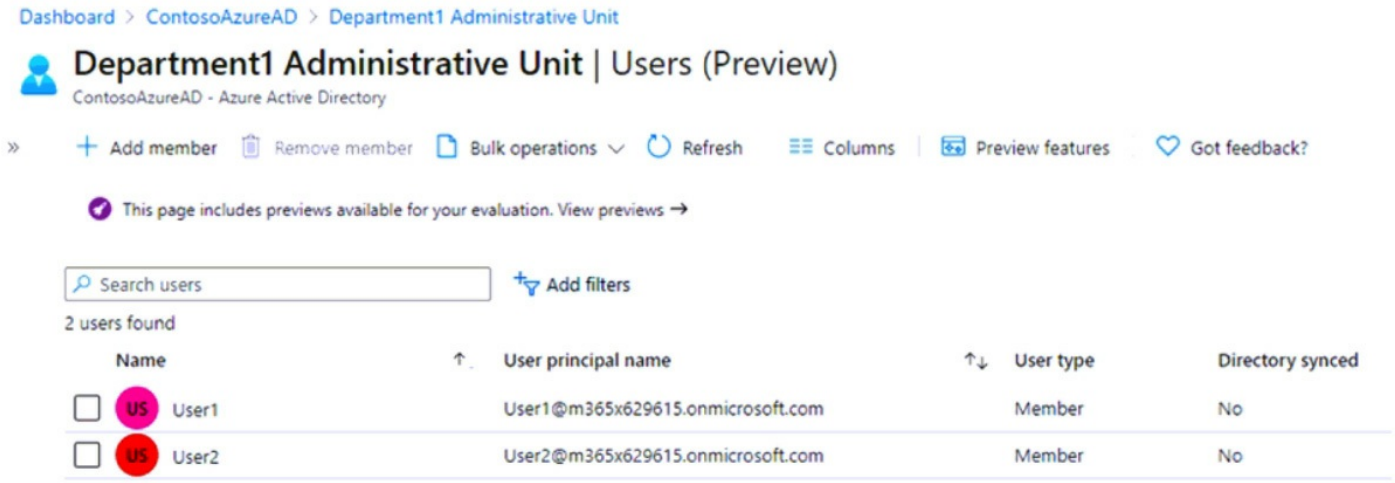
Validating a membership is access review, in my opinion.

Question: 68 CertyIQ

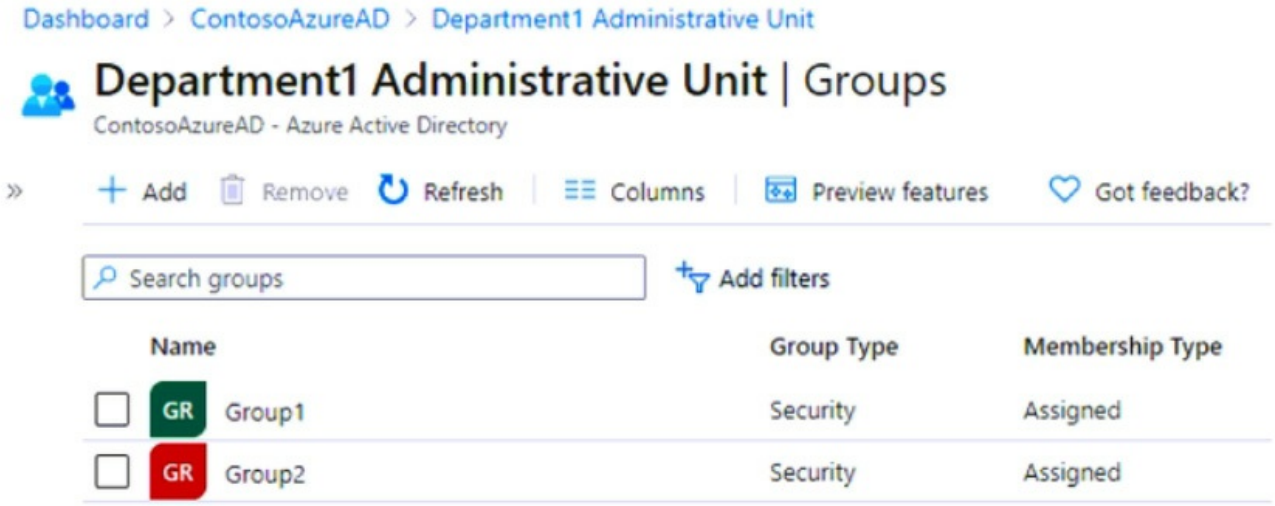
HOTSPOT
-

You have a Microsoft Entra tenant that contains a group named Group3 and an administrative unit named Department1.

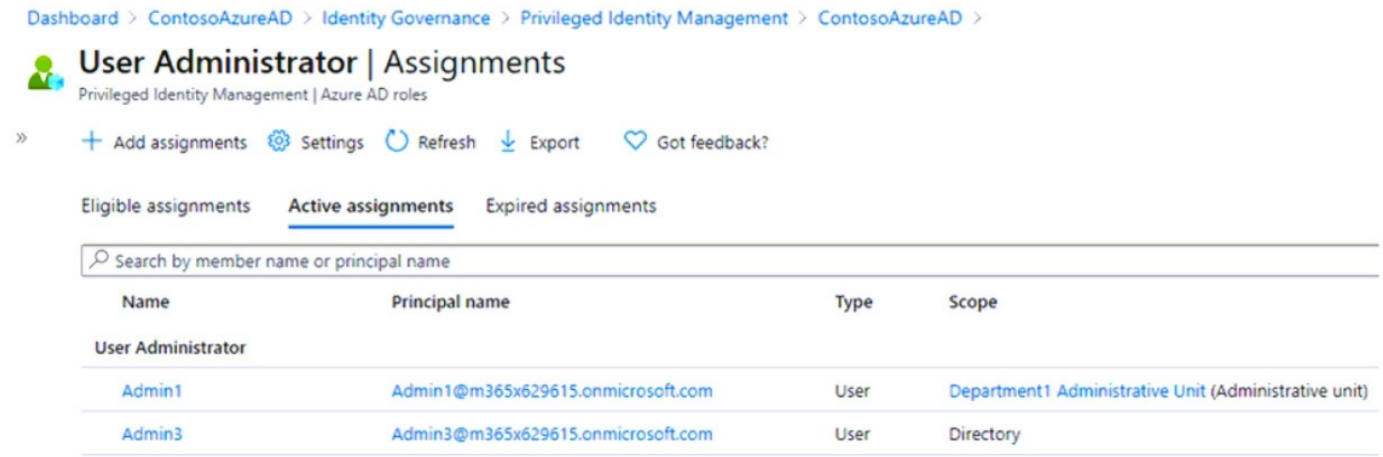
Department1 has the users shown in the Users exhibit. (Click the Users tab.)



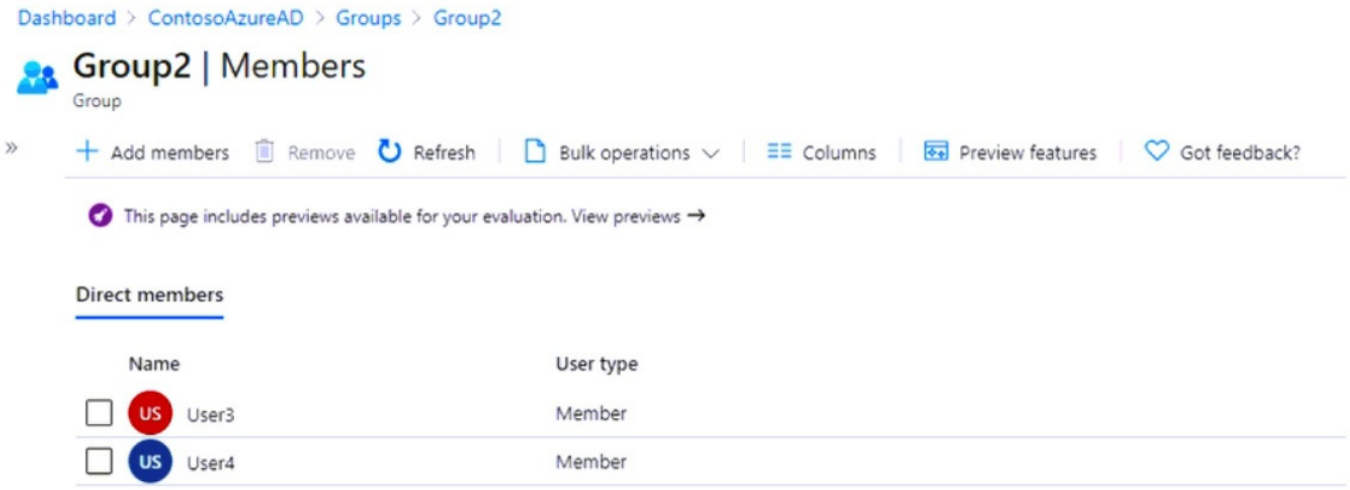
Department1 has the groups shown in the Groups exhibit. (Click the Groups tab.)



The User Administrator role assignments are shown in the Assignments exhibit (Click the Assignments tab.)



The members of Group2 are shown in the Group2 exhibit. (Click the Group2 tab.)



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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Admin1 can reset the passwords of User3 and User4.	○	○
Admin1 can add User1 to Group3.	○	○
Admin3 can reset the password of User1.	○	○

Answer:

Answer Area

Statements	Yes	No
Admin1 can reset the passwords of User3 and User4.	○	○
Admin1 can add User1 to Group3.	○	○
Admin3 can reset the password of User1.	○	○

Explanation:

No

No

Yes

Question: 69 CertyIQ

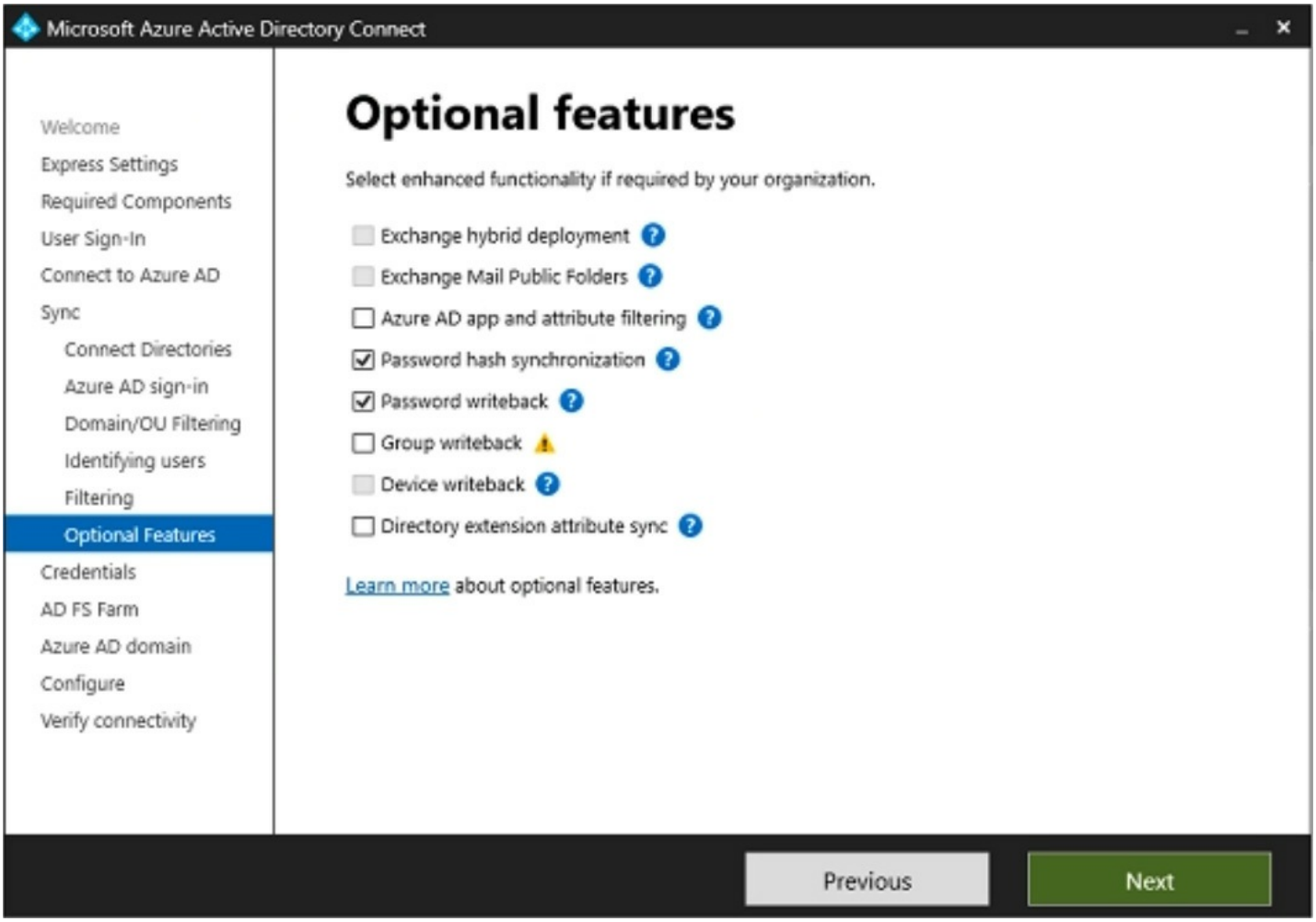
HOTSPOT
-

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.	○	○
User2 can sign in to Server1.	○	○
User3 can sign in to Microsoft 365.	○	○

Answer:

Answer Area

Statements	Yes	No
You can add User1 to Group1.	○	◉
User2 can sign in to Server1.	○	◉
User3 can sign in to Microsoft 365.	◉	○

Explanation:

No

No

yes

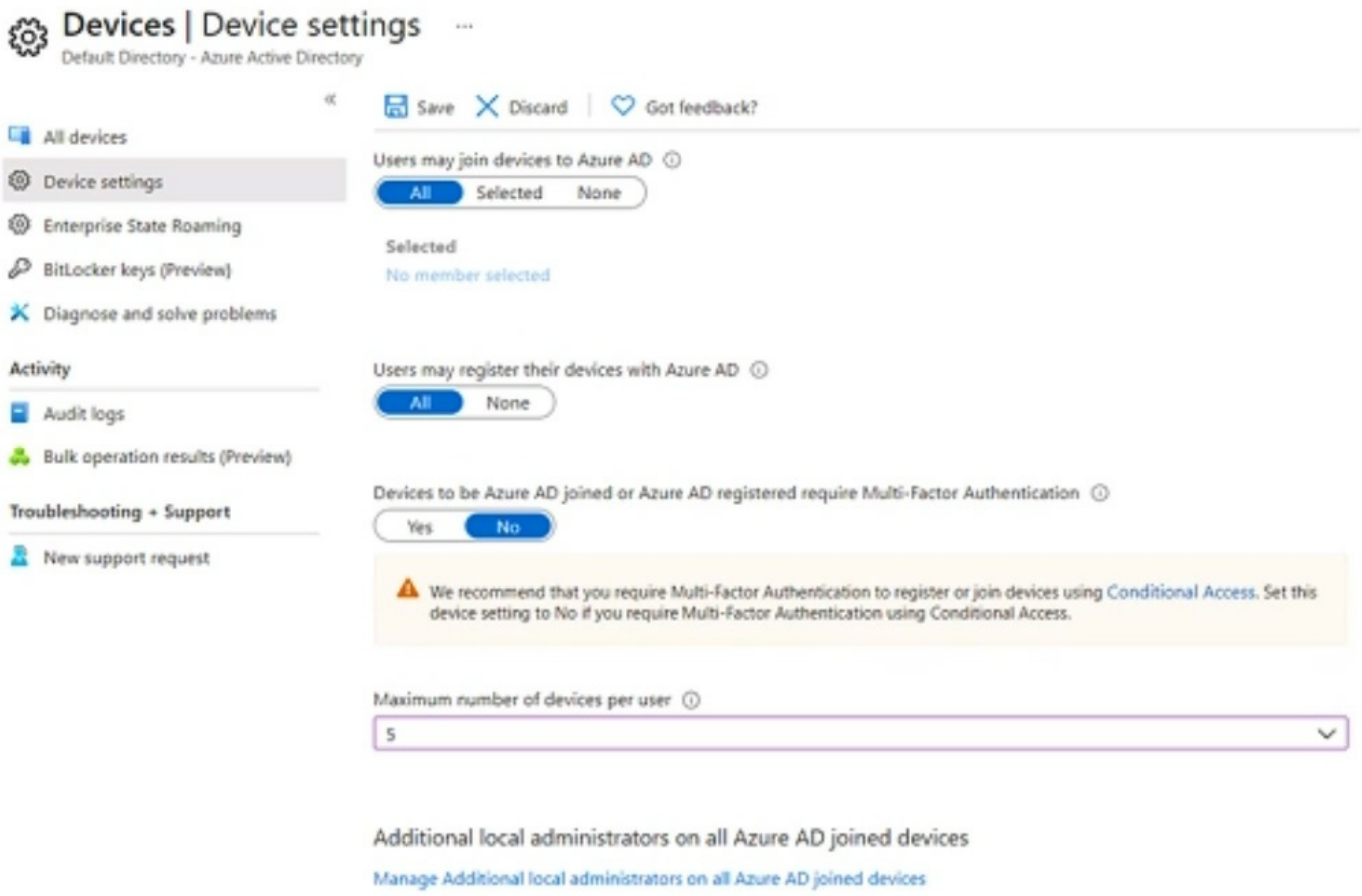
Question: 70 CertyIQ

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.



User1 has the devices shown in the following table.

Name	Operating system	Device identity
Device1	Windows 10	Microsoft Entra joined
Device2	iOS	Microsoft Entra registered
Device3	Windows 10	Microsoft Entra registered
Device4	Android	Microsoft Entra registered

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can join four additional Windows 10 devices to Microsoft Entra ID.	○	○
Admin1 can set Devices to be Microsoft Entra joined or Microsoft Entra registered require Multi-Factor Authentication to **Yes**.	○	○
Admin2 is a local administrator on Device3.	○	○

Answer:

Answer Area

Statements	Yes	No
User1 can join four additional Windows 10 devices to Microsoft Entra ID.	○	○
Admin1 can set Devices to be Microsoft Entra joined or Microsoft Entra registered require Multi-Factor Authentication to **Yes**.	○	○
Admin2 is a local administrator on Device3.	○	○

Explanation:

No

Yes

No

Question: 71 CertyIQ

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

Answer: B

Explanation:

Correct answer is B:Billing Administrator.

Question: 72 CertyIQ

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

Answer: A

Explanation:

Correct answer is A:1.

Question: 73 CertyIQ

You work for a company named Contoso, Ltd. that has a Microsoft Entra tenant named contoso.com.

Contoso is working on a project with the following two partner companies:

•A company named A. Datum Corporation that has a Microsoft Entra tenant named adatum.com.
•A company named Fabrikam, Inc. that has a Microsoft Entra tenant named fabrikam.com.

When you attempt to invite a new guest user from adatum.com to contoso.com, you receive an error message.

You can successfully invite a new guest user from fabnkam.com to contoso.com.

You need to be able to invite new guest users from adatum.com to contoso.com.

What should you configure?

A.Guest invite settings
B.Verifiable credentials
C.Named locations
D.Collaboration restrictions

Answer: D

Explanation:

Correct answer is D:Collaboration restrictions.

Question: 74 CertyIQ

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

Answer: D

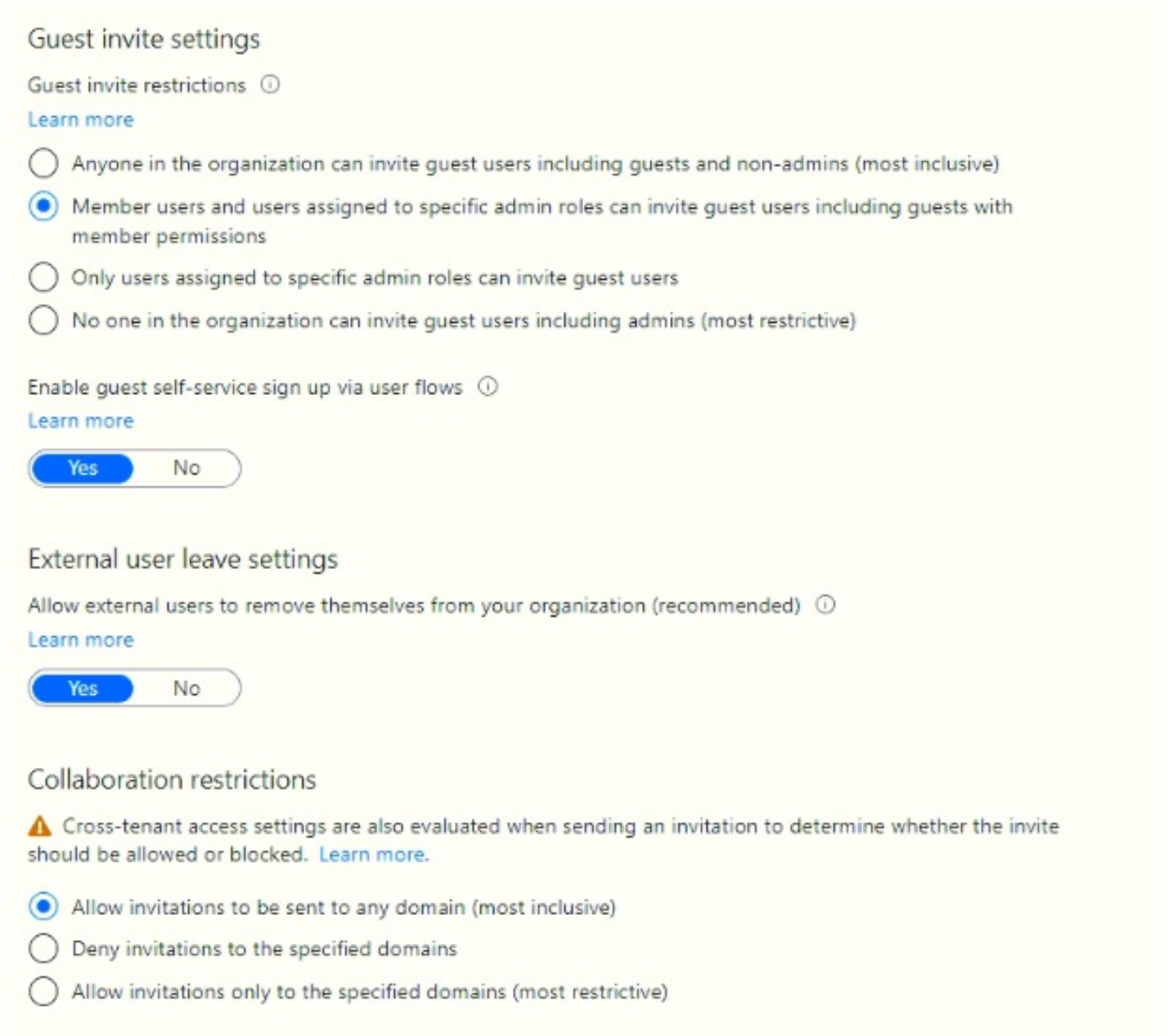
Explanation:

Correct answer is D:VM1, storage1, and WebApp1.

Question: 75 CertyIQ

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.)



The Email one-time passcode for guests setting is enabled for the tenant.

A user named 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

Answer: B

Explanation:

Here=bsmith@fabrikam.com.

Correct answer is B: User2 only.

Question: 76 CertyIQ

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

Answer: C

Explanation:

C. the Set-MgUserLicense cmdletTo 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.

Question: 77 CertyIQ

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

Answer: A

Explanation:

A. the Licenses blade in the Microsoft Entra admin centerTo 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.

Question: 78 CertyIQ

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.

Answer: B

Explanation:

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

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults

Question: 79 CertyIQ

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

Answer: D

Explanation:

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

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordless

Question: 80 CertyIQ

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

Answer: C

Explanation:

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

Question: 81 CertyIQ

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

Answer: D

Explanation:

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

Question: 82 CertyIQ

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

Answer: C

Explanation:

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**

This is not worded properly enough. In CA, if you go into session controls and select 'User conditional access app control', you can monitor or block downloads. However, both of those are in preview and the test doesn't ask you about that. You can select custom policy there https://docs.microsoft.com/en-gb/defender-cloud-apps/proxy-intro-aad#supported-apps-and-clients . SO I say it must be C.

Question: 83 CertyIQ

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

Answer: C

Explanation:

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.

Question: 84 CertyIQ

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

Answer: D

Explanation:

The AzureAD Password Protection proxy service initiates an outbound connection (Port 443) to Azure to pull the banned password list.

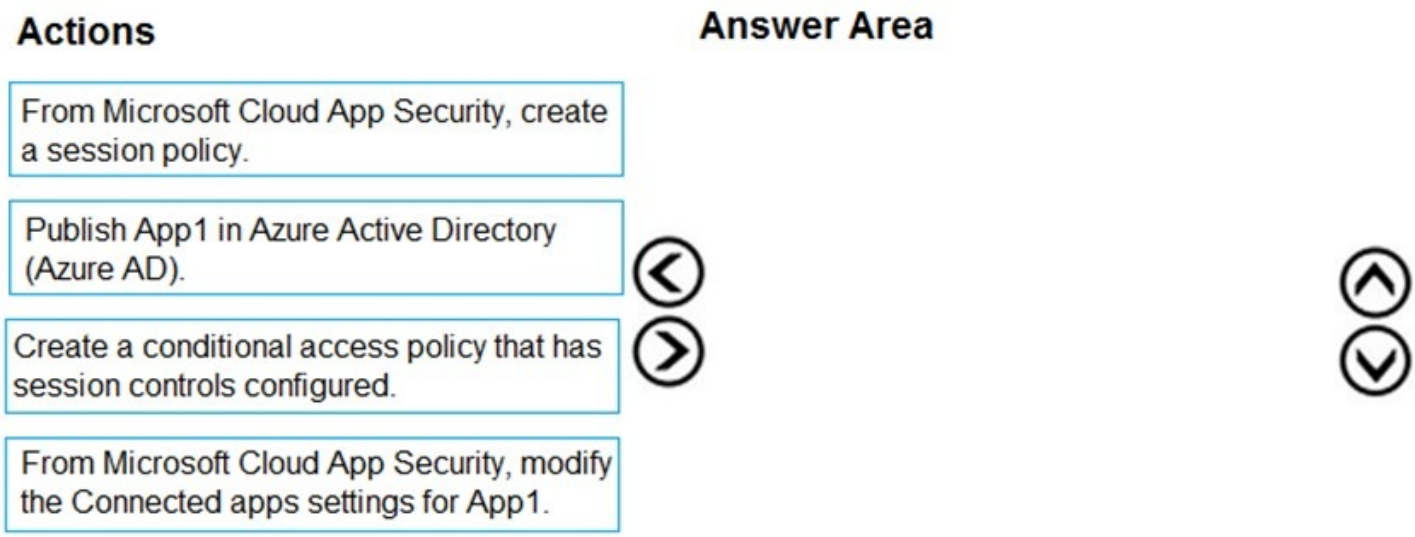
The downloaded banned password list is pulled by the agent installed on DCs.

Reference:

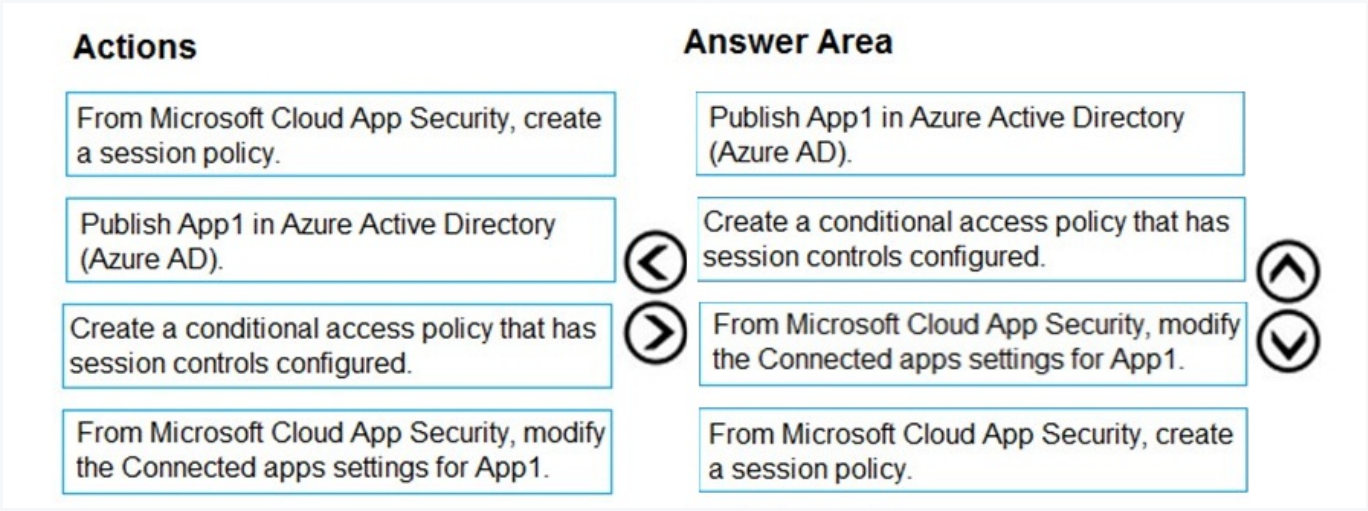
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-deploy

Question: 85 CertyIQ

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:



Answer:



Explanation:

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

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

Question: 86 CertyIQ

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

Answer: C

Explanation:
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

Question: 87 CertyIQ

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

Answer: B

Explanation:

You need to configure the fraud alert settings.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings

Question: 88 CertyIQ

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

Answer: B

Explanation:

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

Question: 89 CertyIQ

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

Answer: B

Explanation:

You need to configure the fraud alert settings.

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.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings

Question: 90 CertyIQ

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

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

Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks

Question: 91

CertyIQ

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

Name	Role
User1	Conditional Access administrator
User2	Authentication administrator
User3	Security administrator
User4	Security operator

You plan to implement Azure AD Identity Protection.
Which users can configure the user risk policy, and which users can view the risky users report? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

Configure the user risk policy:

- User3 only
- User3 and User4 only
- User1, User2, and User3 only
- User1, User3, and User4 only
- User1, User2, User3, and User4

View the risky users report:

- User3 only
- User3 and User4 only
- User1, User2, and User3 only
- User1, User3, and User4 only
- User1, User2, User3, and User4

Answer:

Answer Area

Explanation:

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

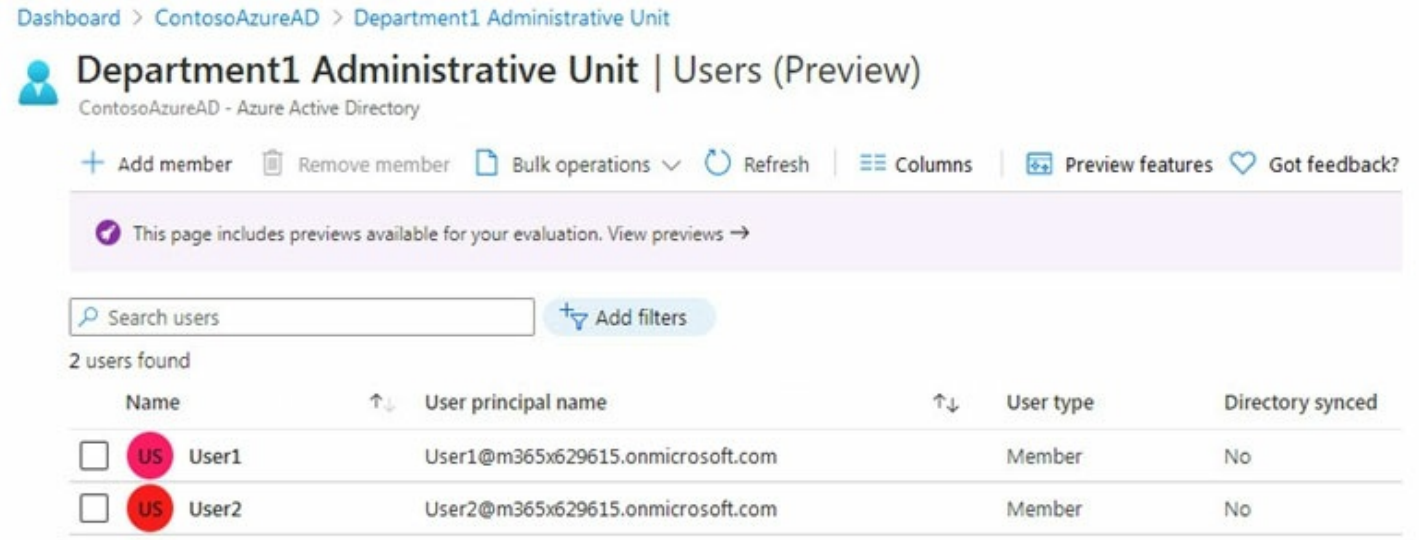
- Grants access to Risky Users Report

Reference:

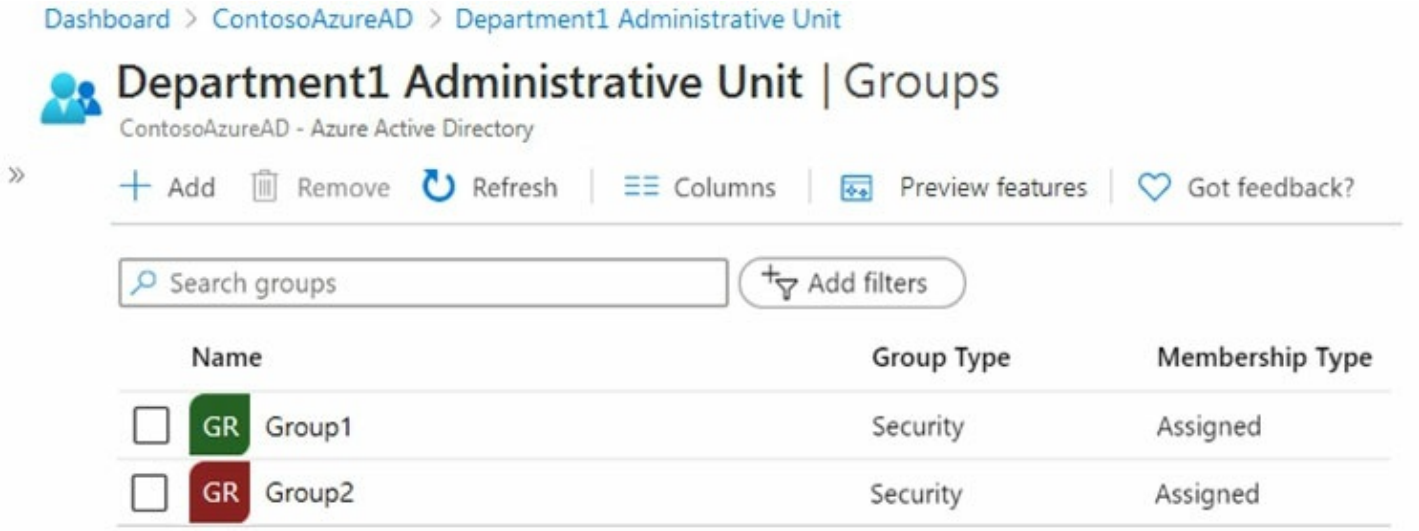
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection

Question: 92 CertyIQ

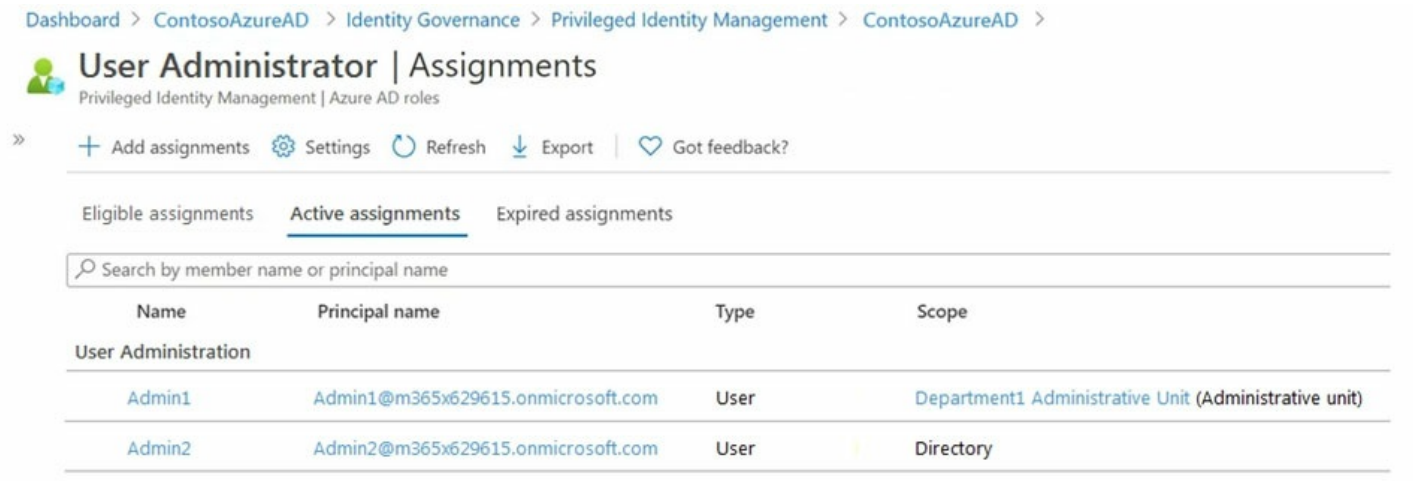
HOTSPOT -
You have an Azure Active Directory (Azure AD) tenant that contains a group named Group3 and an administrative unit named Department1.
Department1 has the users shown in the Users exhibit. (Click the Users tab.)



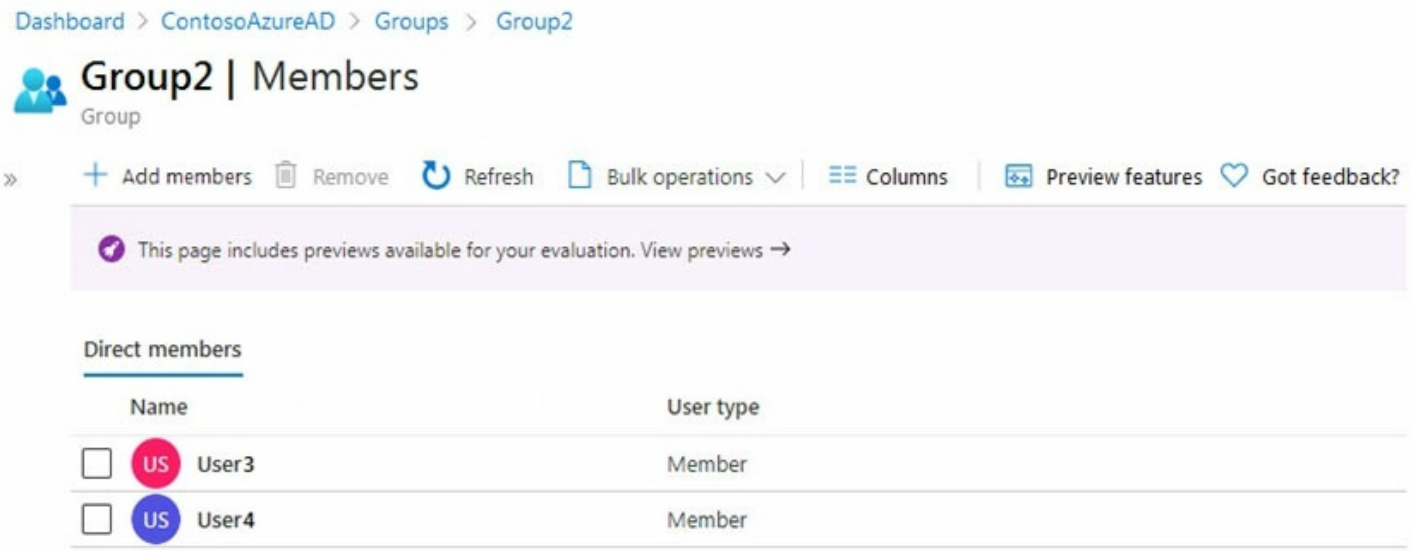
Department1 has the groups shown in the Groups exhibit. (Click the Groups tab.)



Department1 has the user administrator assignments shown in the Assignments exhibit. (Click the Assignments tab.)



The members of Group2 are shown in the Group2 exhibit. (Click the Group2 tab.)



For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

Statements	Yes	No
Admin1 can reset the passwords of User3 and User4.	○	○
Admin1 can add User1 to Group 2	○	○
Admin 2 can reset the password of User1.	○	○

Answer:

Answer Area

Statements	Yes	No
Admin1 can reset the passwords of User3 and User4.	○	○
Admin1 can add User1 to Group 2	○	○
Admin 2 can reset the password of User1.	○	○

Explanation:

#1: N

Because user 3,4 are nested and from G2

See below from;

https://docs.microsoft.com/en-us/azure/active-directory/roles/administrative-units

"A scoped role assignment doesn't apply to members of groups added to an administrative unit, unless the group members are directly added to the administrative unit. For more information, see Add members to an administrative unit."

#2: Y

User Admin have the following attributes

"microsoft.directory/groups/members/update"

Which can be confirmed;

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

#3: Y, User1, is a direct member for the admin unit

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/roles/administrative-units

Question: 93 CertyIQ

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

Answer: A

Explanation:
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

Question: 94 CertyIQ

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

Answer: D

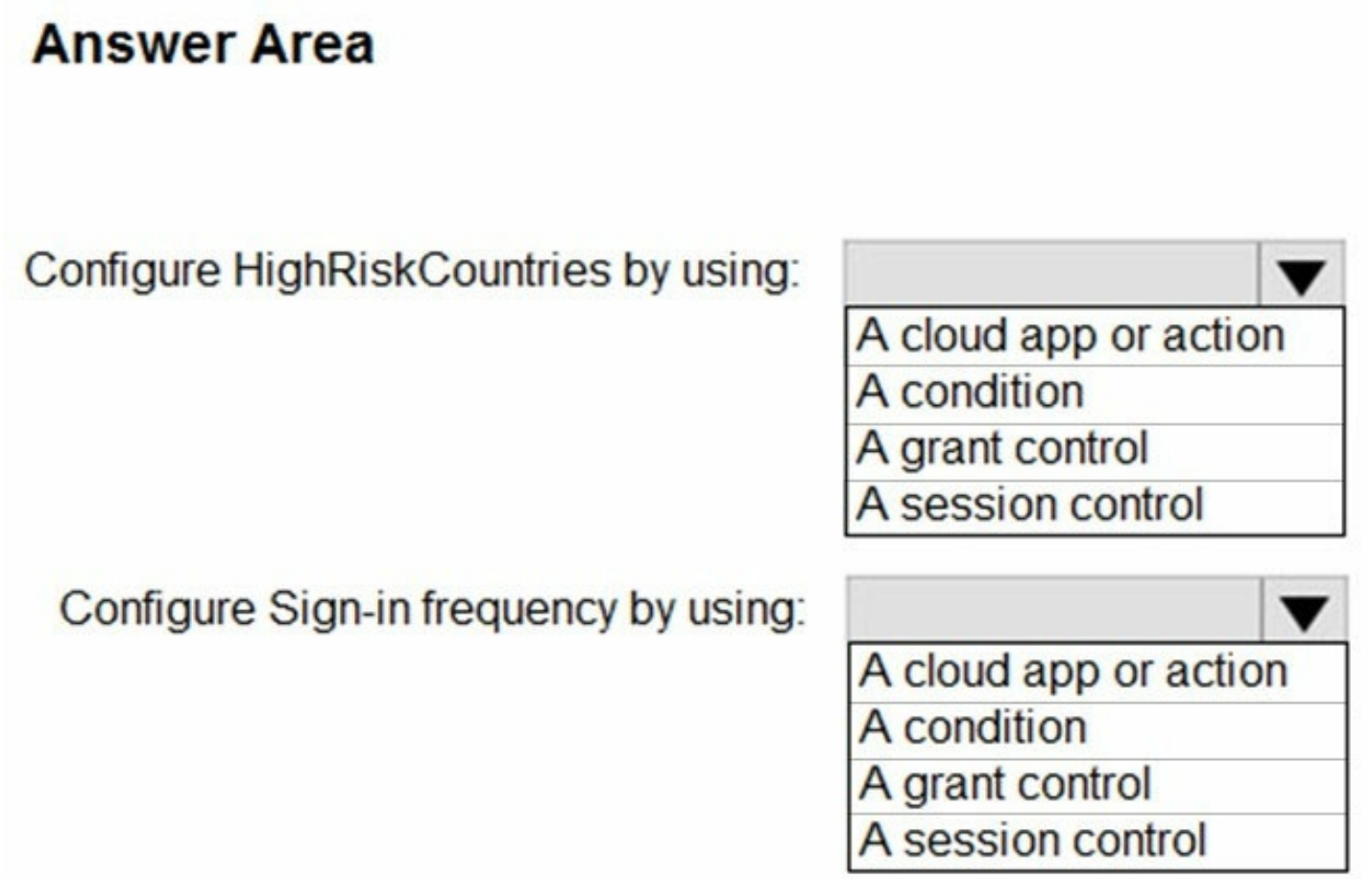
Explanation:
The Authenticator app can be used as a software token to generate an OATH verification code. After entering your username and password, you enter the code provided by the Authenticator app into the sign-in interface.
Incorrect Answers:
A: A notification through the Microsoft Authenticator app requires connectivity to send the verification code to the device requesting the logon.
B: An email requires network connectivity.
C: Security questions are not used as an authentication method but can be used during the self-service password reset (SSPR) process.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-authenticator-app#verification-code-from-mobile-app

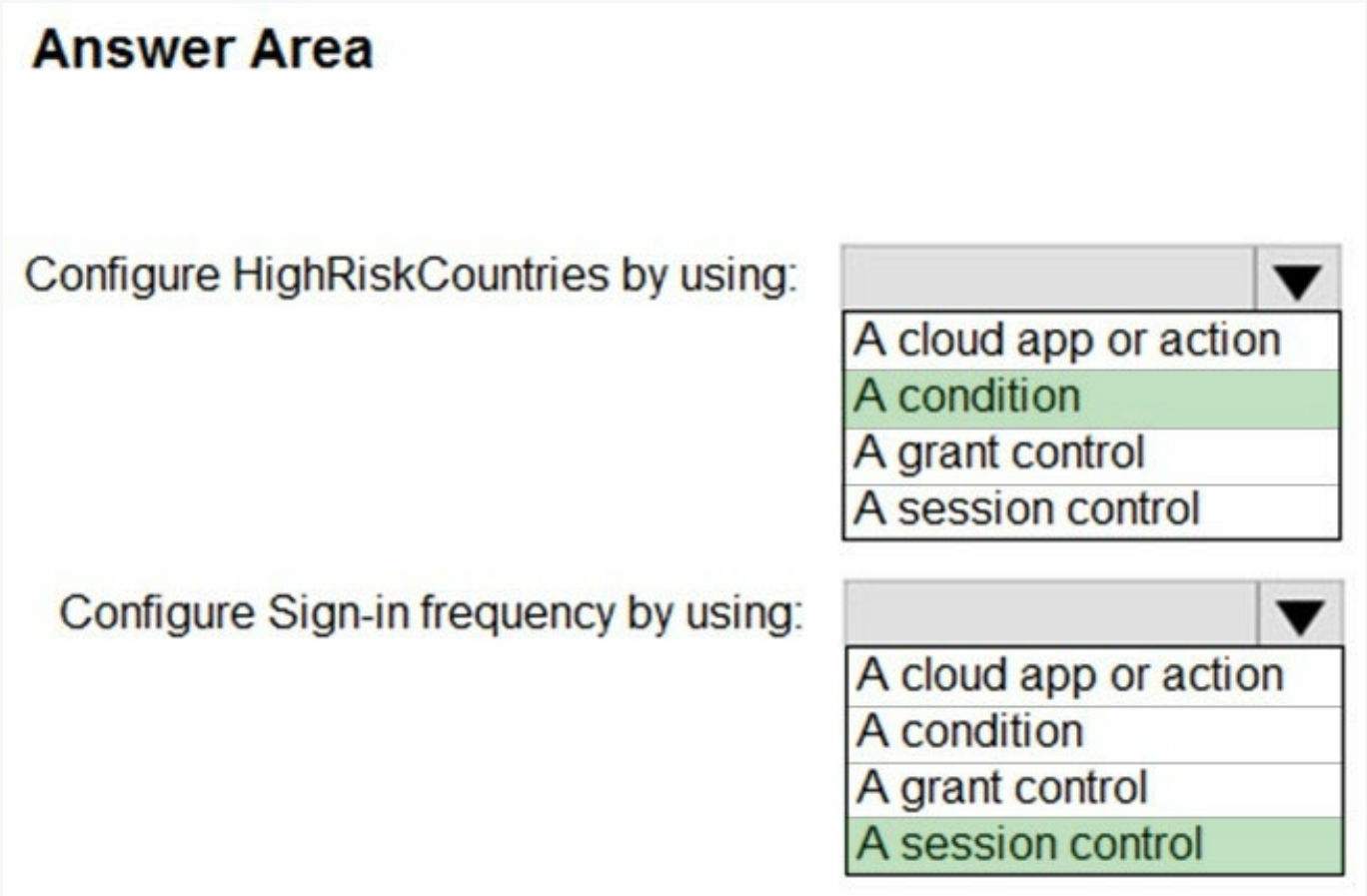
Question: 95 CertyIQ

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:



Explanation:

CONDITION-->named LOCATION.

SESSION-->SIGN-IN FREQUENCY

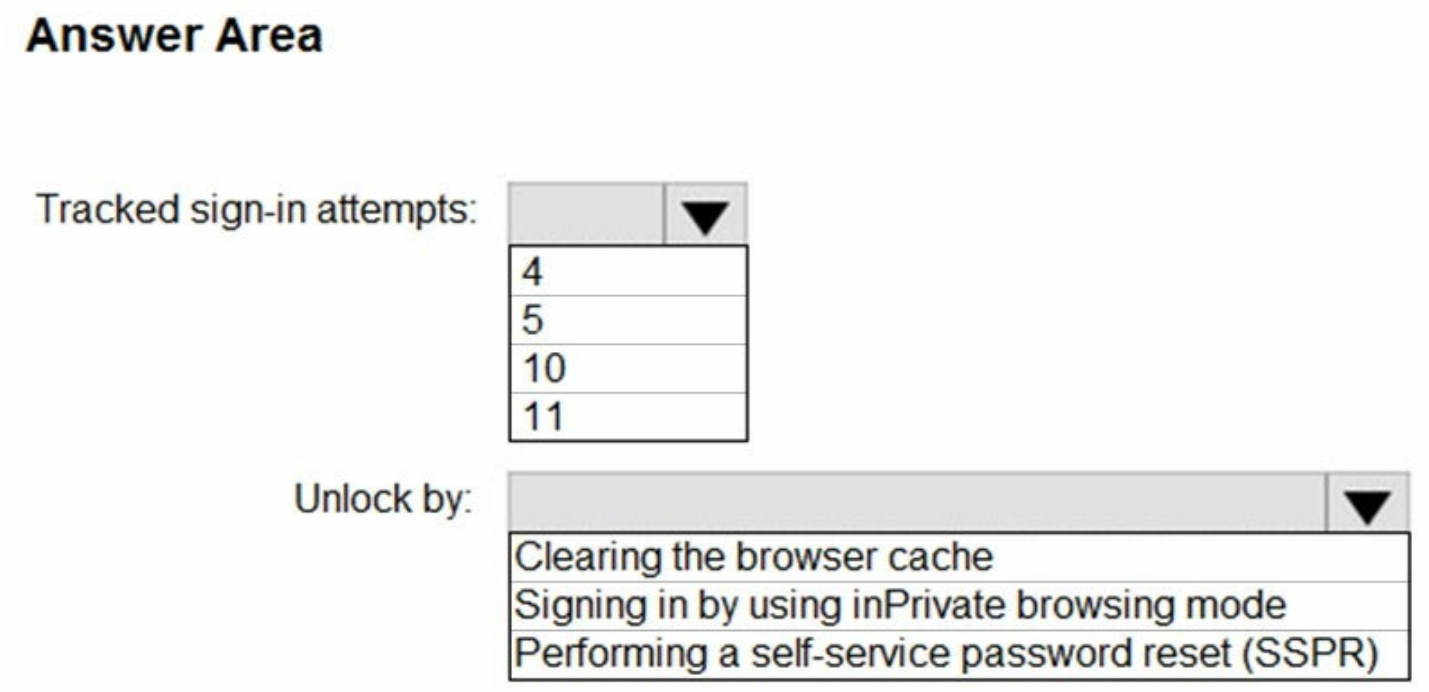
Reference:

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

Question: 96 CertyIQ

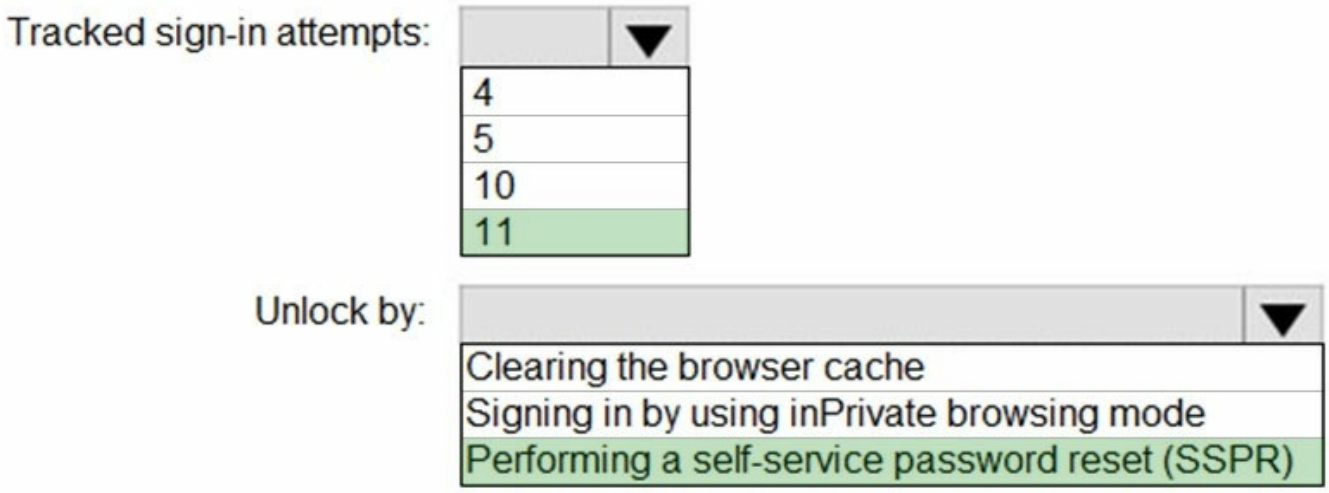
HOTSPOT -
A user named User1 attempts to sign in to the tenant by entering the following incorrect passwords:
- Pa55w0rd12
- Pa55w0rd12
- Pa55w0rd12
- Pa55w.rd12
- Pa55w.rd123
- Pa55w.rd123
- Pa55w.rd123
- Pa55word12
- Pa55word12
- Pa55word12
- Pa55w.rd12

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:

Answer Area

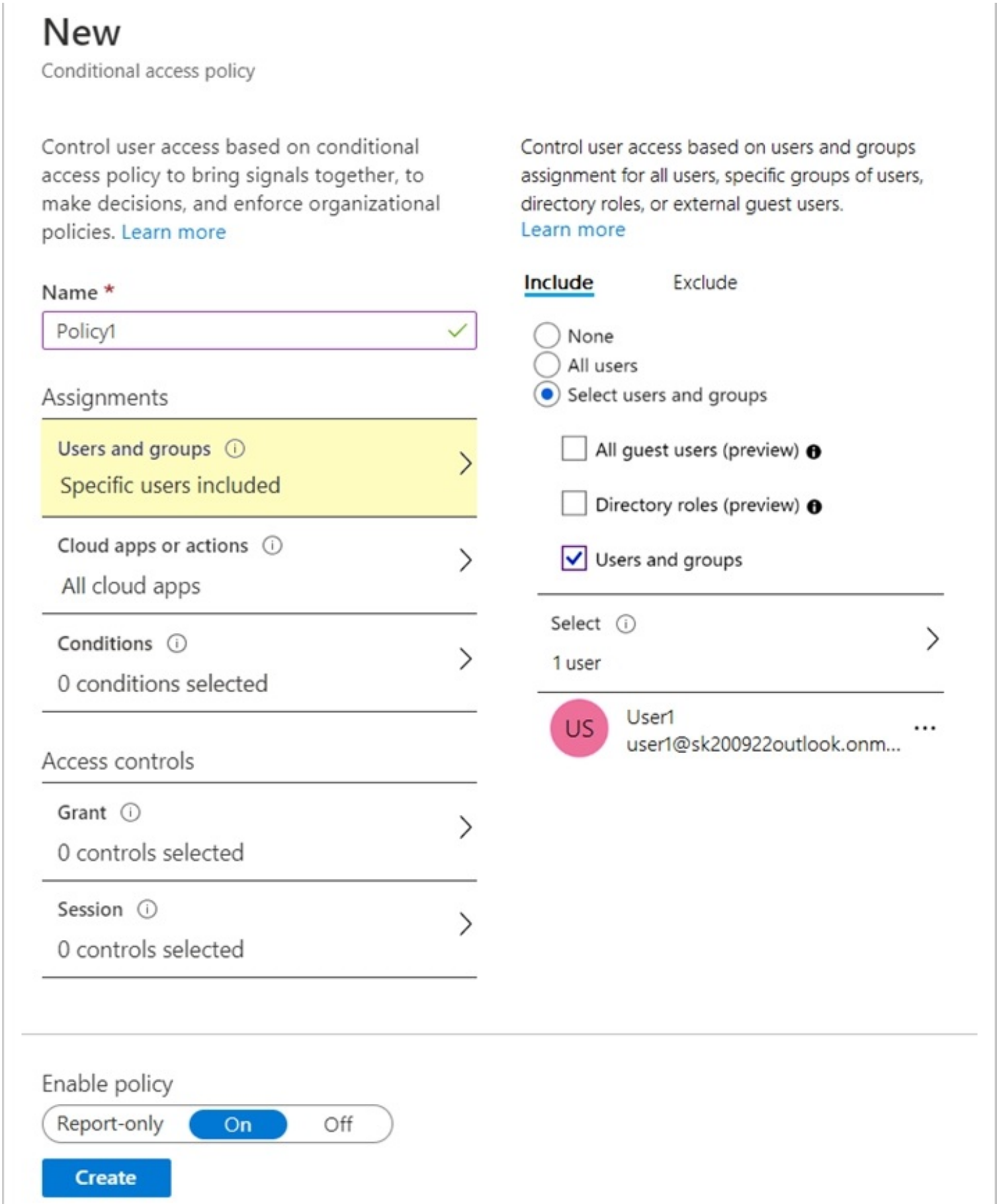


Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment

Question: 97 CertyIQ

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.



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:

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

Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-all-users-mfa

Question: 98 CertyIQ

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

Answer: A

Explanation:

A

In details:

Privileged Auth Admin can reset passwords of non admins and admin accounts

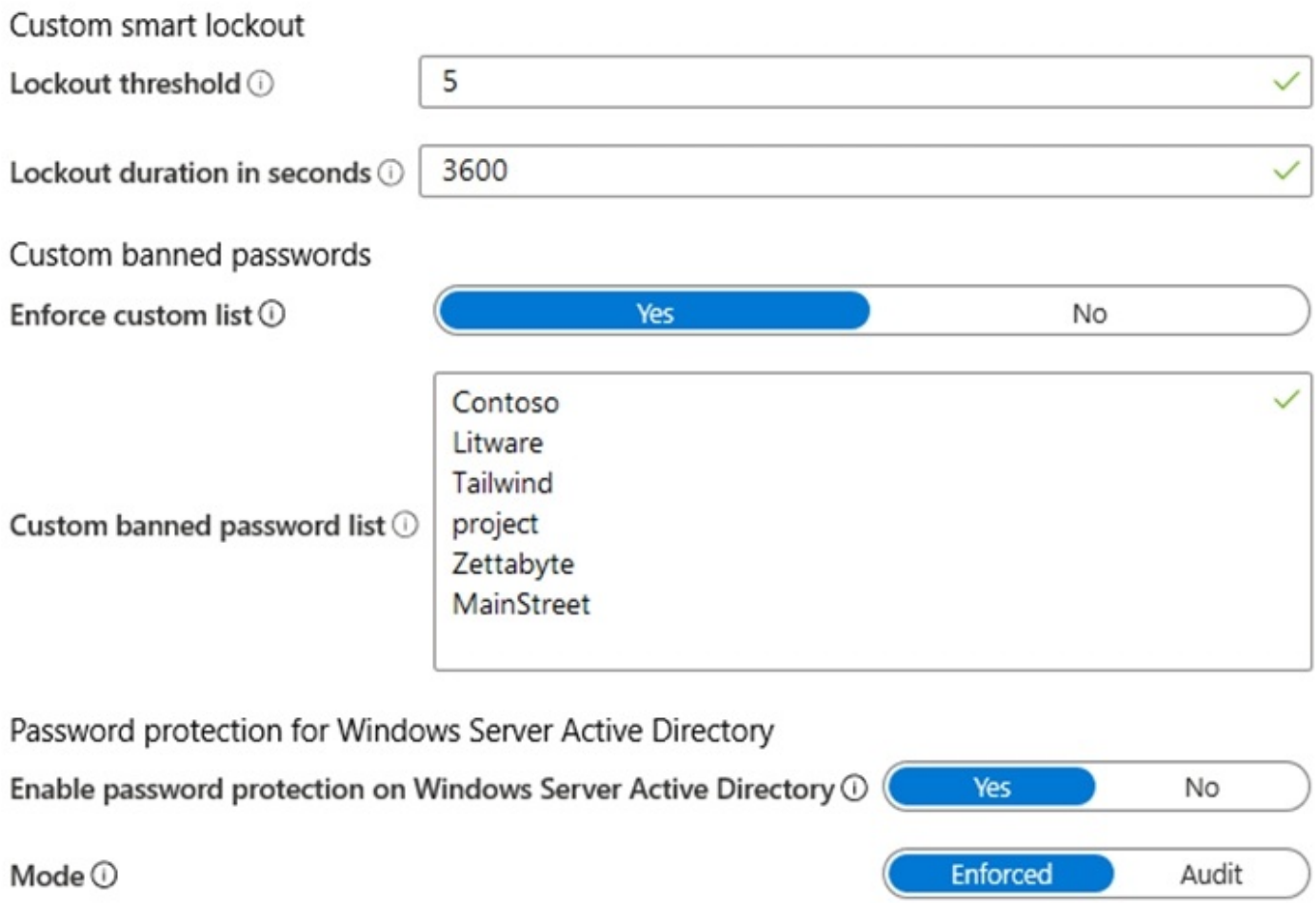
Helpdesk Admins can reset non admins and Helpdesk Admins password

Authentication Administrator can only reset non admin accounts password

To follow the least privilege requirement, Authentication Administrator should be the answer

Question: 99 CertyIQ

You configure Azure Active Directory (Azure AD) Password Protection as shown in the exhibit. (Click the Exhibit tab.)



You are evaluating the following passwords:
-
-
- C0nt0s0

Which passwords will be blocked?

A. and only
B. C0nt0s0 only
C. C0nt0s0, , and
D. C0nt0s0 and only
E. C0nt0s0 and only

Answer: C

Explanation:

Full Question Correction:

You are evaluating the following passwords:

✑ Pr0jectlitw@re

✑ T@ilw1nd

✑ C0nt0s0

Which passwords will be blocked?

A. Pr0jectlitw@re and T@ilw1nd only

B. C0nt0s0 only

C. C0nt0s0, Pr0jectlitw@re, and T@ilw1nd

D. C0nt0s0 and T@ilw1nd only

E. C0nt0s0 and Pr0jectlitw@re only

Correct Answer= C

Reference:

https://blog.enablingtechcorp.com/azure-ad-password-protection-password-evaluation

Question: 100

CertyIQ

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

Answer: A

Explanation:
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

Question: 101 CertyIQ

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

Name	Role
User1	Security administrator
User2	Privileged authentication administrator
User3	Service support administrator

User2 reports that he can only configure multi-factor authentication (MFA) to use the Microsoft Authenticator app.
You need to ensure that User2 can configure alternate MFA methods.
Which configuration is required, and which user should perform the configuration? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

Configuration:
- Enable access reviews.
- Enable Azure AD Privileged Identity Management (PIM).
- Modify security defaults.

User:
- User1 only
- User2 only
- User3 only
- User1 and User2 only
- User1 and User3 only
- User2 and User3 only

Answer:

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

Explanation:

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

Question: 102 CertyIQ

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

Answer: C

Explanation:
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

Question: 103 CertyIQ

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.

Answer: B

Explanation:

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

Question: 104 CertyIQ

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

Name	Member of	Multi-factor authentication (MFA)
User1	Group1	Enabled but never used
User2	Group2	Disabled
User3	Group1, Group2	Enforced and used

In Azure. AD Identity Protection, you configure a user risk policy that has the following settings:
✑ Assignments:
- Users: Group1
- User risk: Low and above
✑ Controls:
- Access: Block access
✑ Enforce policy: On
In Azure AD Identify Protection, you configure a sign-in risk policy that has the following settings:
✑ Assignments:
- Users: Group2
- Sign-in risk: Low and above
✑ Controls:
- Access: Require multi-factor authentication
✑ Enforce policy: On
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:

Statements	Yes	No
User1 can sign in from an anonymous IP address.	○	○
User2 can sign in from an anonymous IP address.	○	○
User3 can sign in from an anonymous IP address.	○	○

Answer:

Statements	Yes	No
User1 can sign in from an anonymous IP address.	○	○
User2 can sign in from an anonymous IP address.	○	○
User3 can sign in from an anonymous IP address.	○	○

Explanation:

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

Question: 105

CertyIQ

You have an Azure Active Directory (Azure AD) tenant.
You configure self-service password reset (SSPR) by using the following settings:
- Require users to register when signing in: Yes
- Number of methods required to reset: 1

What is a valid authentication method available to users?

A. an email to an address outside your organization

B. a smartcard

C. an FID02 security token

D. a Microsoft Teams chat

Answer: A

Explanation:
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

Question: 106 CertyIQ

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

Answer: A

Explanation:
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

Question: 107 CertyIQ

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

Answer: C

Explanation:
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

Question: 108 CertyIQ

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

Answer: C

Explanation:

App Passwords are a legacy feature for old Office versions. Windows Hello is the way to go.

Question: 109 CertyIQ

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)

Answer: A

Explanation:
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

Question: 110 CertyIQ

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

Name	Member of	Multi-factor authentication (MFA)
User1	Group1	Disabled
User2	Group2	Enforced

You have the locations shown in the following table.

Name	Private address space	Public NAT address space
Location1	10.10.0.0/16	20.93.15.0/24
Location2	192.168.0.0/16	193.17.17.0/24

The tenant contains a named location that has the following configurations:
- Name: Location1
- Mark as trusted location: Enabled

IPv4 range: 10.10.0.0/16 -

MFA has a trusted IP address range of 193.17.17.0/24.
- Name: CAPolicy1
- Assignments
- Users or workload identities: Group1
- Cloud apps or actions: All cloud apps
- Conditions
- Locations: All trusted locations
- Access controls
- Grant
- Grant access: Require multi-factor authentication
- Session: 0 controls selected
- Enable policy: On

For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:

Statements	Yes	No
If User1 connects to the tenant from IP address 10.10.0.150, the user will be prompted for MFA.	○	○
If User2 connects to the tenant from IP address 10.10.1.160, the user will be prompted for MFA.	○	○
If User2 connects to the tenant from IP address 192.168.1.20, the user will be prompted for MFA.	○	○

Answer:

Statements	Yes	No
If User1 connects to the tenant from IP address 10.10.0.150, the user will be prompted for MFA.	○	●
If User2 connects to the tenant from IP address 10.10.1.160, the user will be prompted for MFA.	●	○
If User2 connects to the tenant from IP address 192.168.1.20, the user will be prompted for MFA.	○	●

Explanation:

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: 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)

Box 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)

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings

Question: 111 CertyIQ

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:

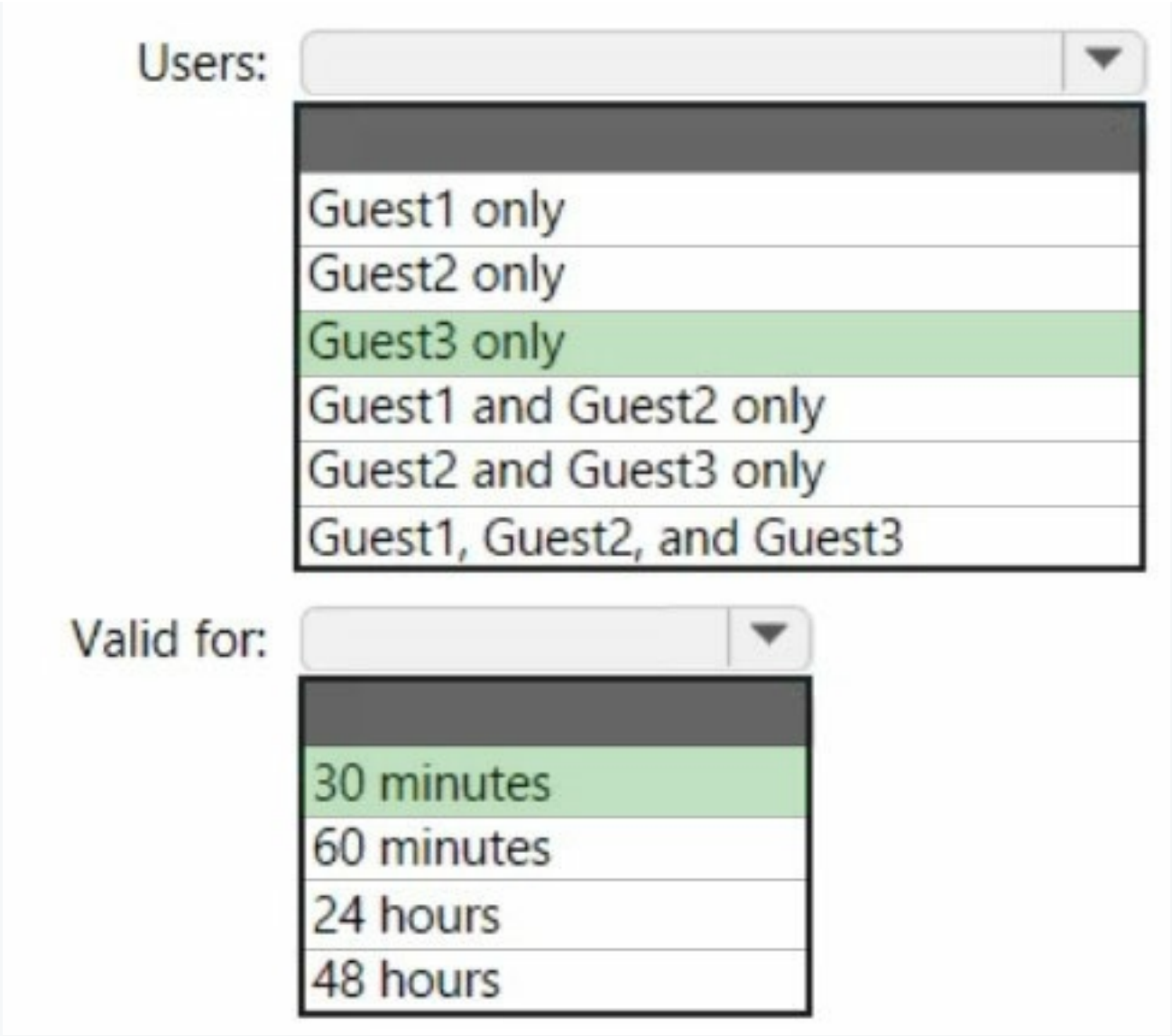
Users:

- 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

Answer:



Explanation:
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

Question: 112 CertyIQ

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

Answer: B

Explanation:

https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacy-authentication

Question: 113 CertyIQ

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

Answer: A

Question: 114 CertyIQ

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

Answer: C

Explanation:

The answer is correct. C. tested in the lab. You can clone Role2 (CustomRole) and Azure Built-in Roles

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

Question: 115 CertyIQ

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

Answer: A

Explanation:

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.

Question: 116 CertyIQ

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

Answer: B

Explanation:

Windows Hello for Business

Question: 117 CertyIQ

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:

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.	○	◉

Explanation:

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

Question: 118

CertyIQ

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:

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.	○	○

Explanation:

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

Question: 119 CertyIQ

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

Answer: D

Explanation:

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)

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

Question: 120 CertyIQ

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

Answer: B

Explanation:

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.

Question: 121 CertyIQ

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

Answer: A

Explanation:

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

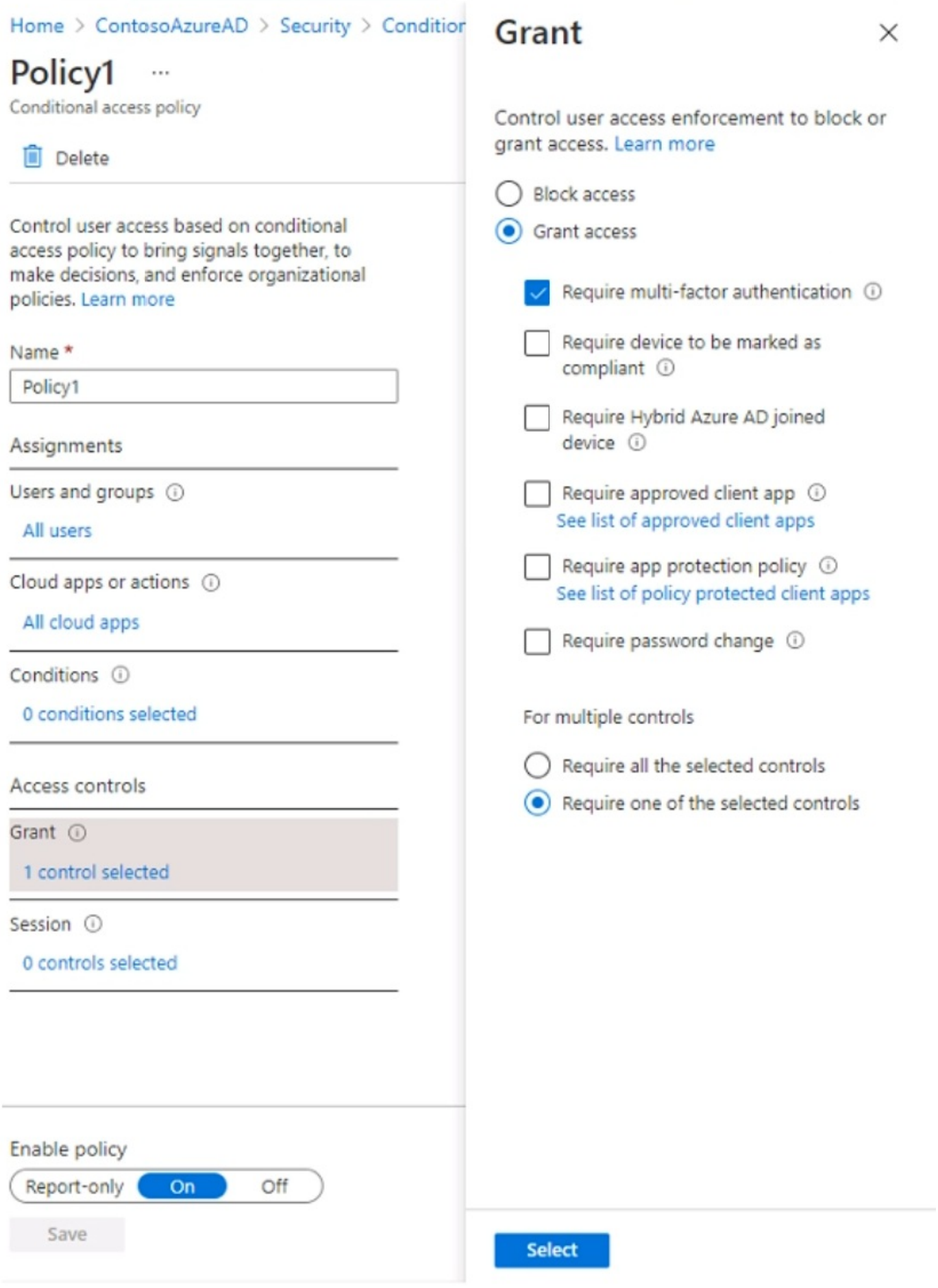
Password spray

Question: 122 CertyIQ

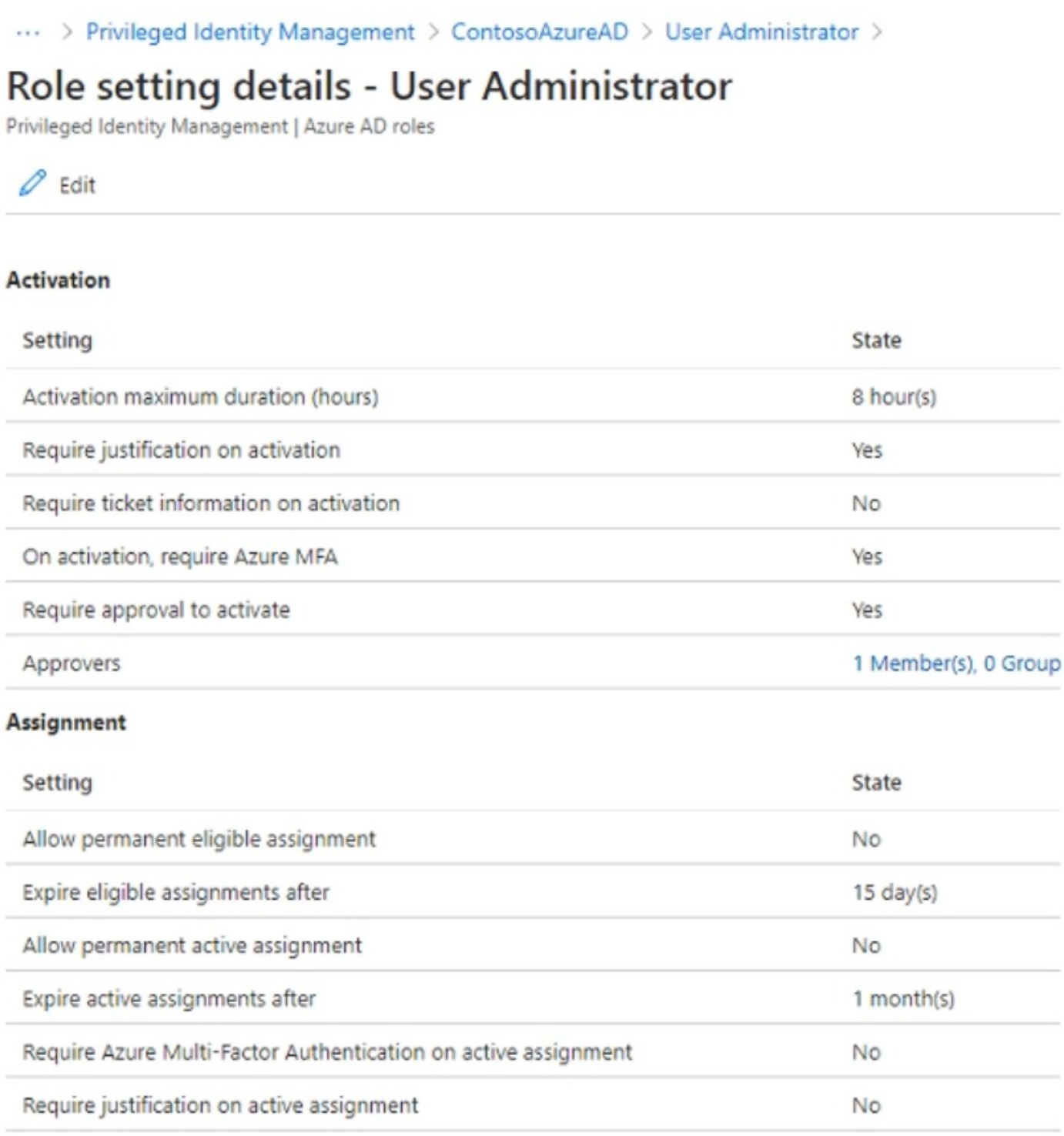
HOTSPOT
-

You have a Microsoft 365 tenant.

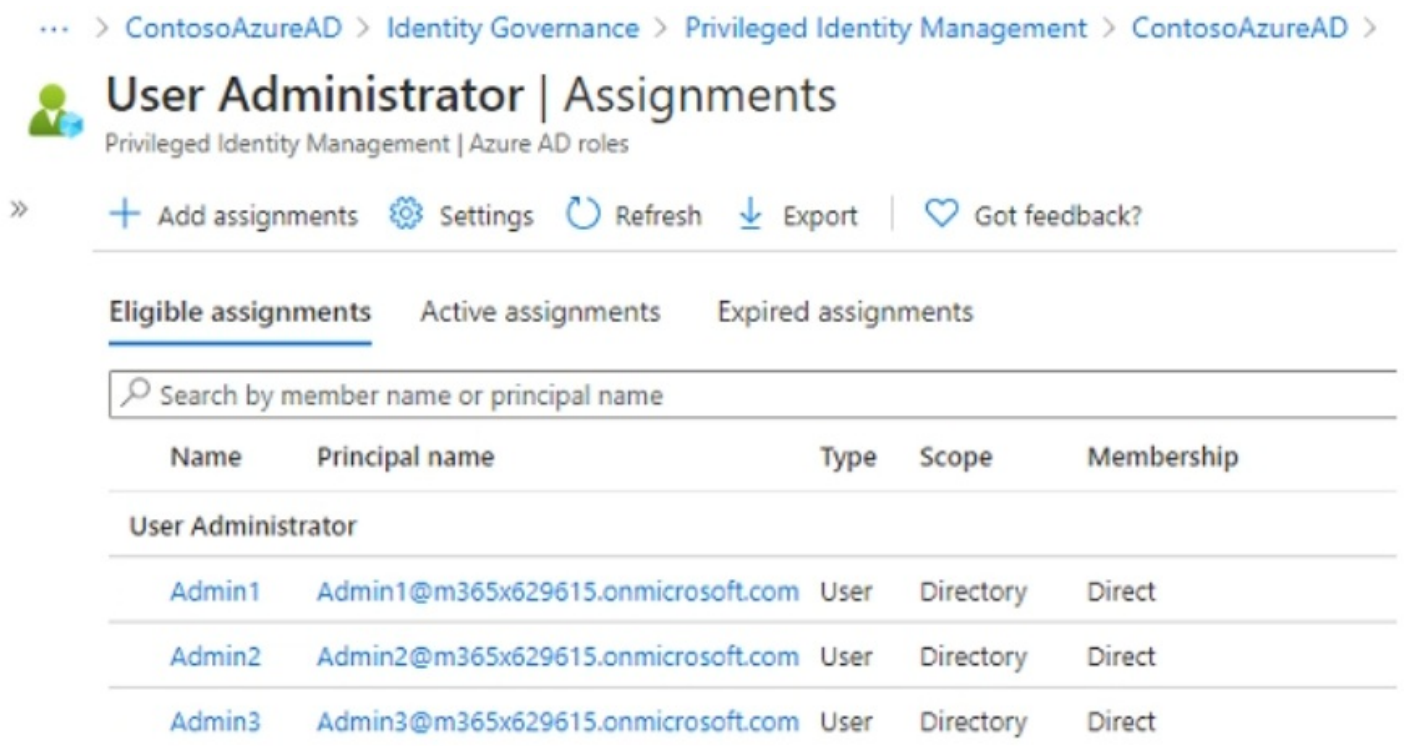
You configure a conditional access policy as shown in the Conditional Access policy exhibit. (Click the Conditional Access policy tab.)



You view the User administrator role settings as shown in the Role setting details exhibit. (Click the Role setting details tab.)



You view the User administrator role assignments as shown in the Role assignments exhibit. (Click the Role assignments tab.)



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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
Before Admin1 can perform a task that requires the User administrator role, an approver must approve the activation request.	○	○
Admin2 can request activation of the User administrator role for a period of two hours.	○	○
If Admin3 connects to the Azure Active Directory admin center, and then activates the User administrator role, Admin3 will be prompted to authenticate by using multi-factor authentication (MFA) twice.	○	○

Answer:

Statements	Yes	No
Before Admin1 can perform a task that requires the User administrator role, an approver must approve the activation request.	○	○
Admin2 can request activation of the User administrator role for a period of two hours.	○	○
If Admin3 connects to the Azure Active Directory admin center, and then activates the User administrator role, Admin3 will be prompted to authenticate by using multi-factor authentication (MFA) twice.	○	○

Question: 123

CertyIQ

HOTSPOT
-

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

Name	User risk level
User1	Low
User2	Medium
User3	High

You have the Azure AD Identity Protection policies shown in the following table.

Type	Users	User risk	Sign-in risk	Controls
User risk policy	All users	Low and above	Unconfigured	Block access
Sign-in risk policy	All users	Unconfigured	High	Block access

You review the Risky users report and the Risky sign-ins report and perform actions for each user as shown in the following table.

User	Action
User1	Confirm user compromised
User2	Confirm sign-in safe
User3	Dismiss user risk
User2	Confirm user compromised

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
User1 can sign in by using multi-factor authentication (MFA).	○	○
User2 can sign in by using multi-factor authentication (MFA).	○	○
User3 can sign in from an anonymous IP address.	○	○

Answer:

Statements	Yes	No
User1 can sign in by using multi-factor authentication (MFA).	○	○
User2 can sign in by using multi-factor authentication (MFA).	○	○
User3 can sign in from an anonymous IP address.	○	○

Explanation:

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/

Question: 124 CertyIQ

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

Answer: D

Explanation:

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

Question: 125 CertyIQ

DRAG DROP
-

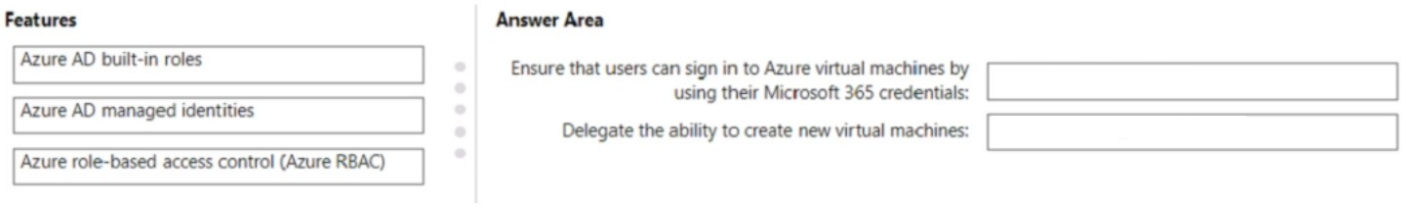
You have a Microsoft 365 E5 subscription and an Azure subscription.

You need to meet the following requirements:

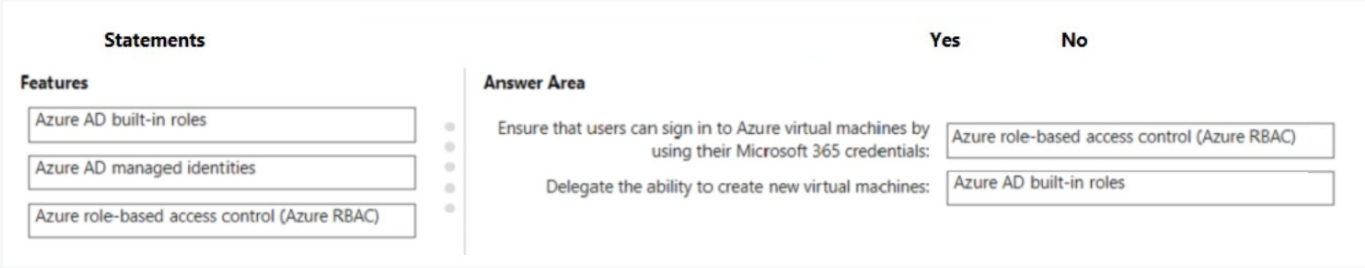
• Ensure that users can sign in to Azure virtual machines by using their Microsoft 365 credentials.
• Delegate the ability to create new virtual machines.

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.



Answer:



Explanation:

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

Question: 126 CertyIQ

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

Answer: D

Explanation:

Windows Hello for Business

Question: 127 CertyIQ

HOTSPOT
-

Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with an Azure AD tenant. The AD DS domain contains the organizational units (OUs) shown in the following table.

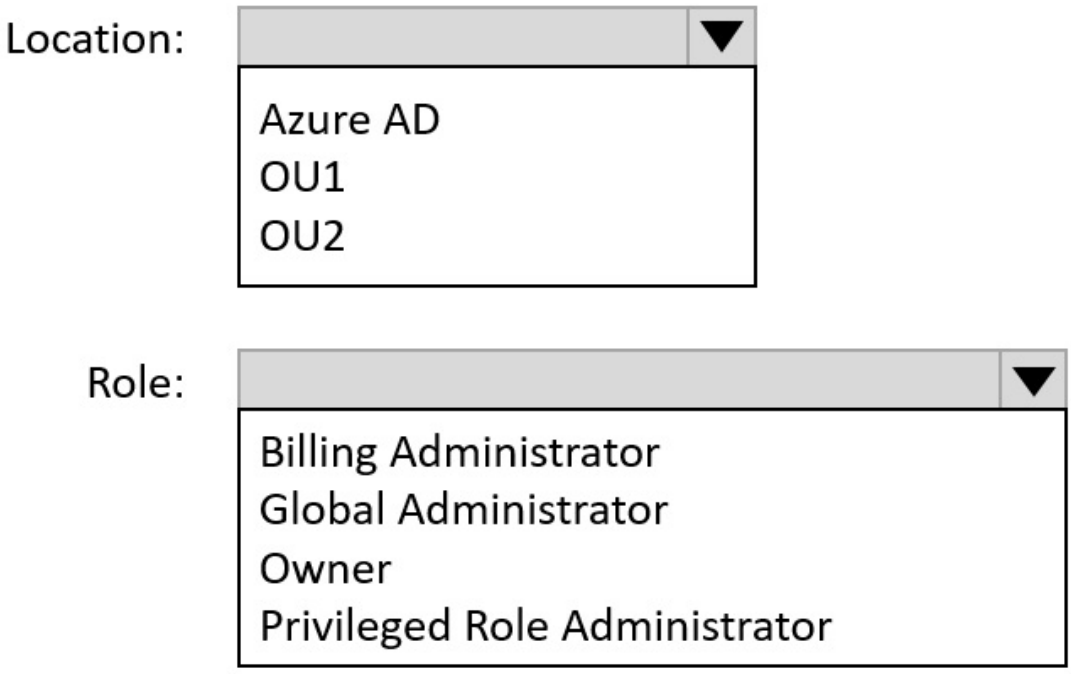
Name	Description
OU1	Syncs with Azure AD
OU2	Does **NOT** sync with Azure AD

You need to create a break-glass account named BreakGlass.

Where should you create BreakGlass, and which role should you assign to BreakGlass? To answer, select the appropriate options in the answer area.

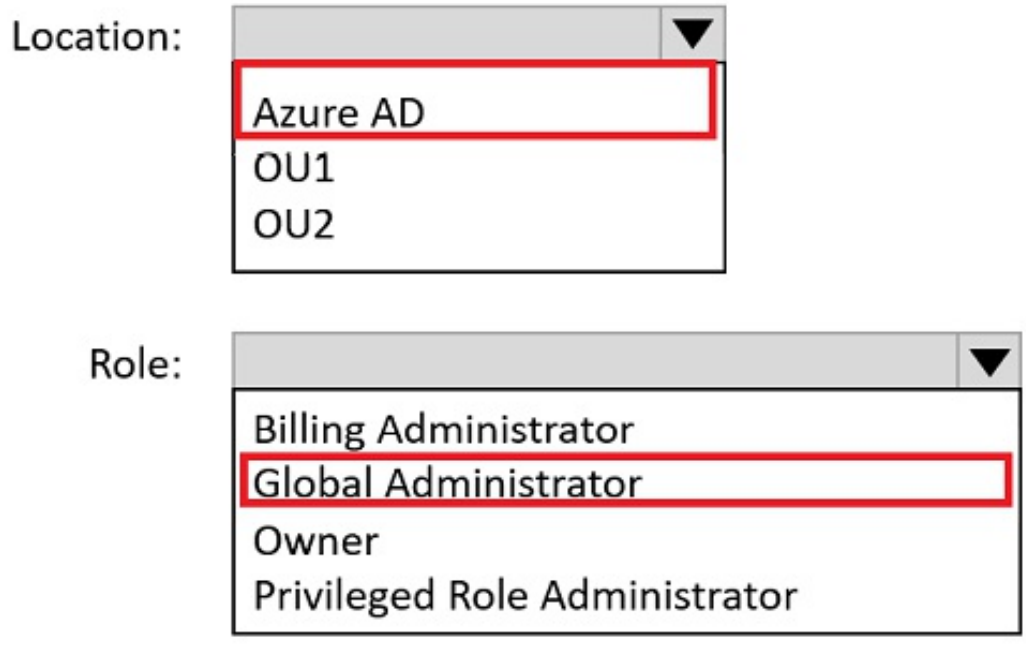
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area



Explanation:

AzureAD and Global Admin

https://learn.microsoft.com/en-us/azure/active-directory/roles/security-emergency-access#how-to-create-an-emergency-access-account

Question: 128 CertyIQ

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.

Answer: B

Explanation:

B (Access Packages) is the correct answer -

https://learn.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-create

Question: 129 CertyIQ

HOTSPOT
-

You have an Azure subscription.

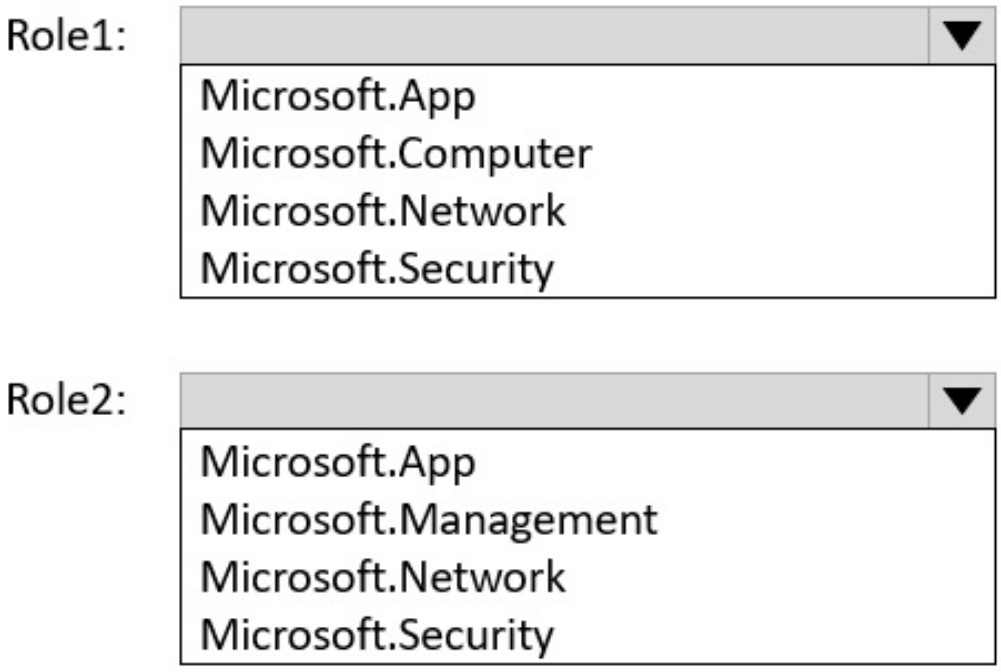
You need to create two custom roles named Role1 and Role2. The solution must meet the following requirements:

•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



Answer:

Answer Area

Explanation:

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

Question: 130 CertyIQ

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

Answer: D

Explanation:

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.

An automated voice call and an SMS requires mobile connectivity.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods

Question: 131 CertyIQ

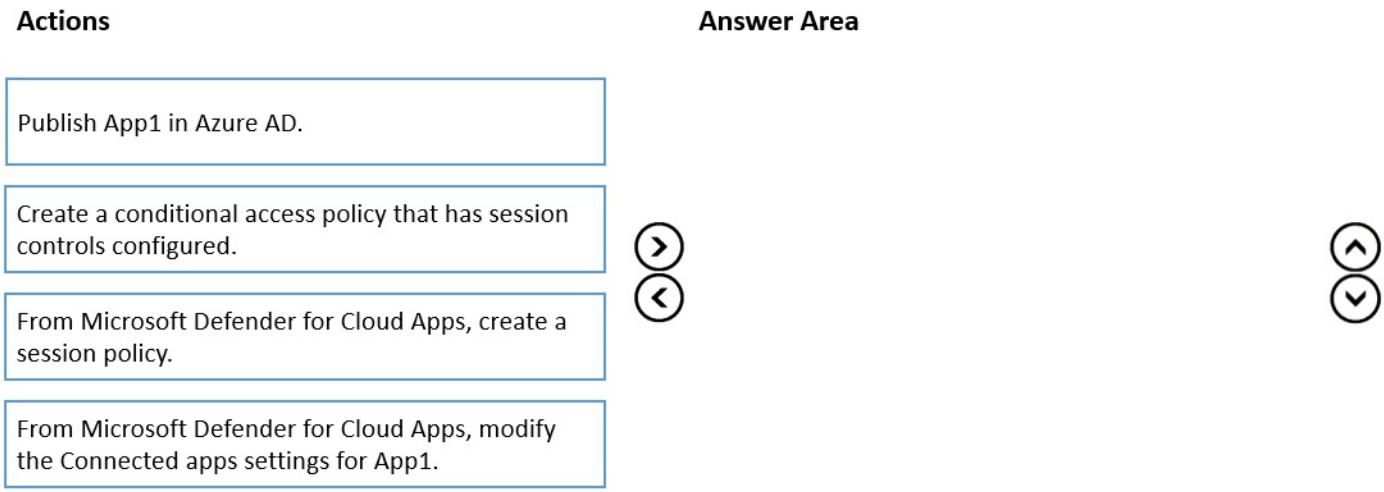
DRAG DROP
-

You have a Microsoft 365 E5 tenant.

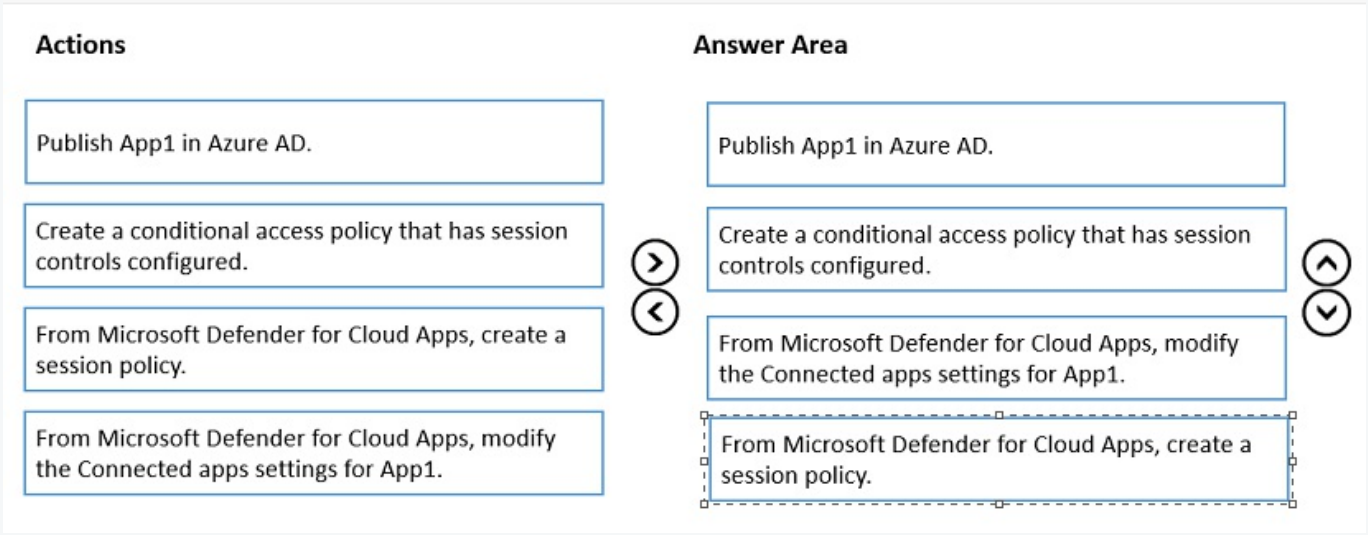
You purchase a cloud app named App1.

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.



Answer:



Explanation:

1. Publish App1.2. Create a conditional access policy that has session controls configured.3. From MCAS modify the Connected apps settings4. From MCAS create a session policyReference - https://techcommunity.microsoft.com/t5/itops-talk-blog/step-by-step-blocking-data-downloads-via-microsoft-cloud-app/ba-p/326357

Question: 132

CertyIQ

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:

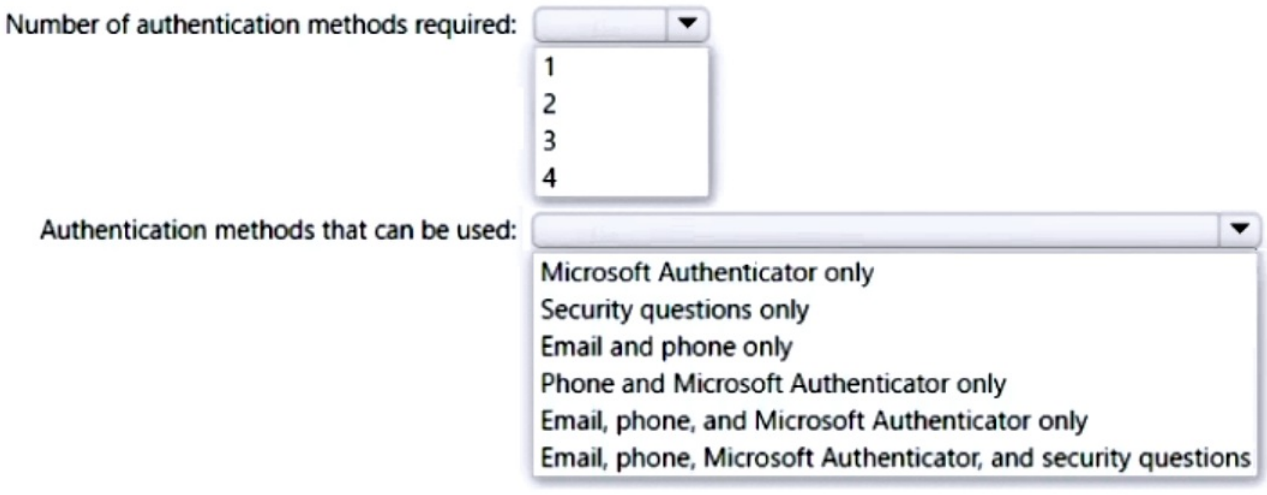
•Users assigned the User administrator role must be able to request permission to use the role when needed for up to one year.
•Users must be prompted to register for MFA and provided with an option to bypass the registration for a grace period.
•Users must provide one authentication method to reset 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.

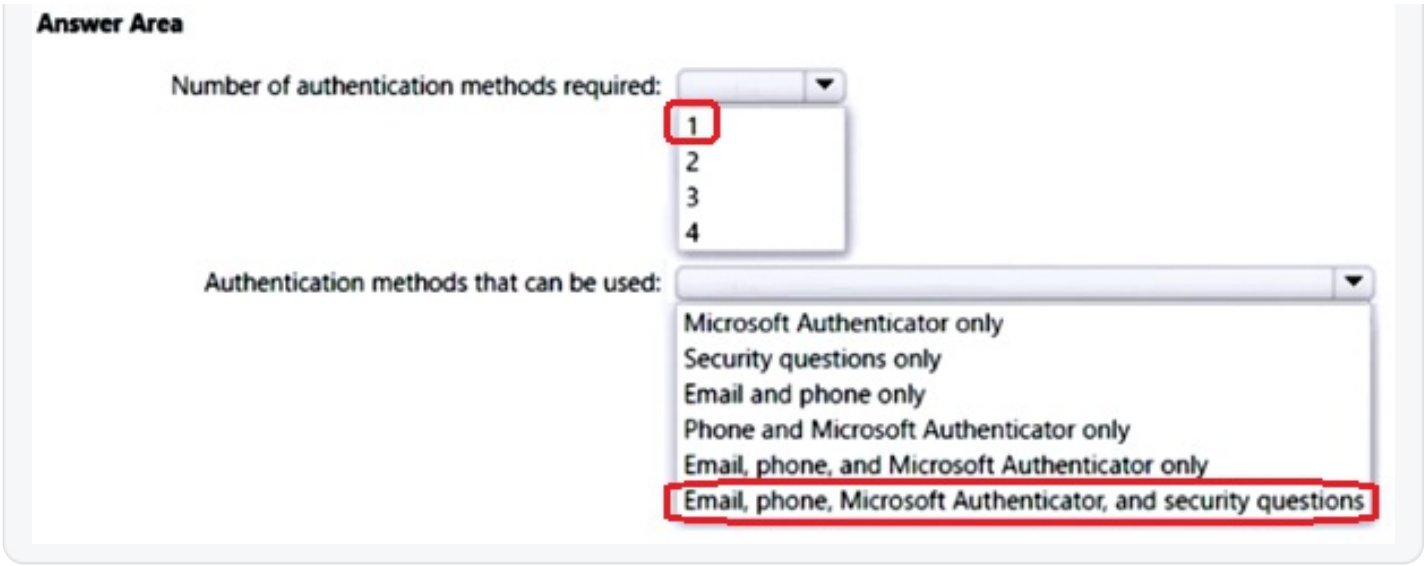
What occurs when User3 attempts to use SSPR? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Answer:



Question: 133 CertyIQ

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:

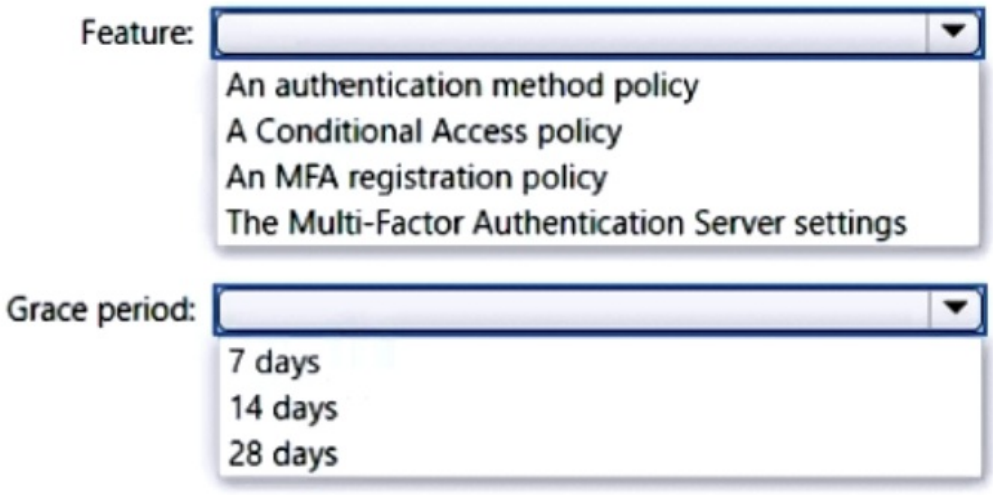
•Users assigned the User administrator role must be able to request permission to use the role when needed for up to one year.
•Users must be prompted to register for MFA and provided with an option to bypass the registration for a grace period.
•Users must provide one authentication method to reset 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



Answer:

Answer Area

Explanation:

Box1: MFA registration policyBox2: 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.

https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-mfa-policy#user-experience

Question: 134

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

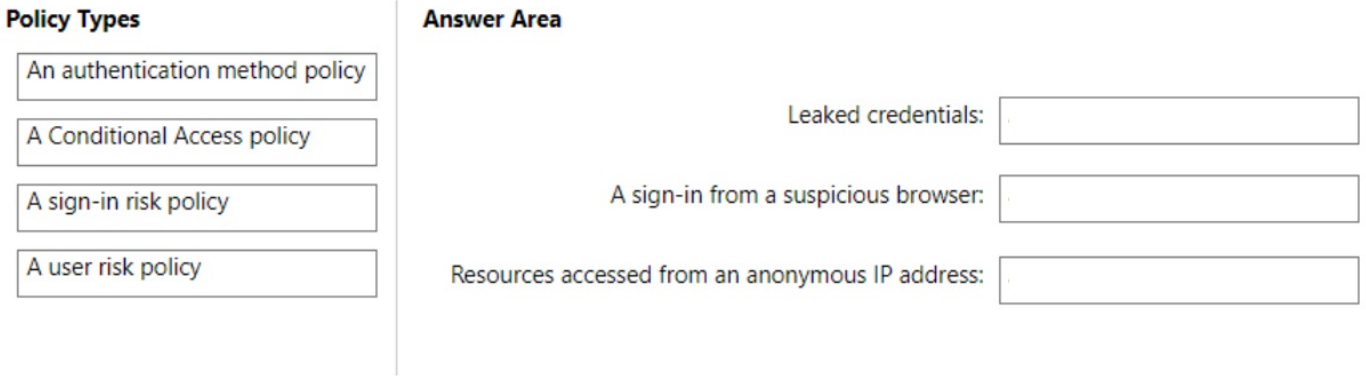
ADatum identifies the following technical requirements:

•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.

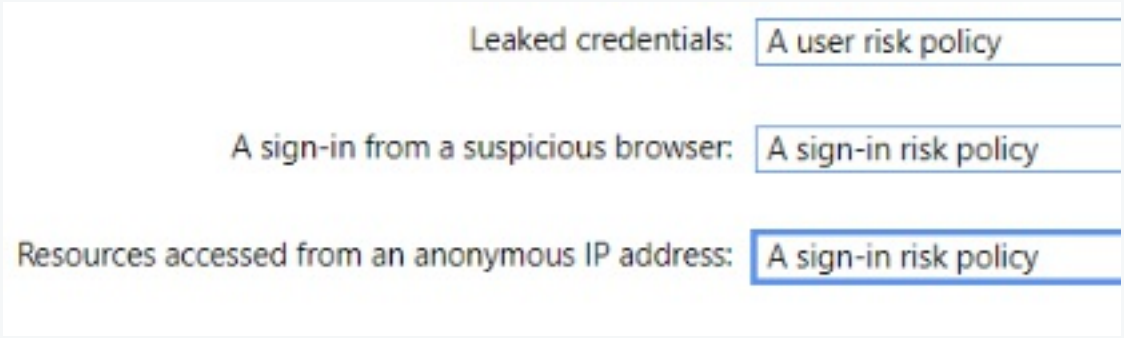
You need to resolve the recent security incident issues.

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.



Answer:



Question: 135 CertyIQ

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

Answer: B

Explanation:

sign-in logs

Question: 136 CertyIQ

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.

Answer: A

Explanation:

https://learn.microsoft.com/en-us/defender-cloud-apps/access-policy-aad

Question: 137 CertyIQ

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

Answer: D

Explanation:

a verification code from the Microsoft Authenticator app

Question: 138 CertyIQ

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

Answer: D

Explanation:

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

Question: 139 CertyIQ

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

You configure self-service password reset (SSPR) by using the following settings:

•Require users to register when signing in: Yes
•Number of methods required to reset: 1

What is a valid authentication method available to users?

A.an email to an address outside your organization
B.a mobile app notification
C.an FIDO2 security token
D.an email to an address in your organization

Answer: A

Explanation:

an email to an address outside your organization

Question: 140 CertyIQ

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

Answer: B

Explanation:

Correct answer is B:a mobile app code.

Reference:

https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks#authentication-methods

Question: 141 CertyIQ

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

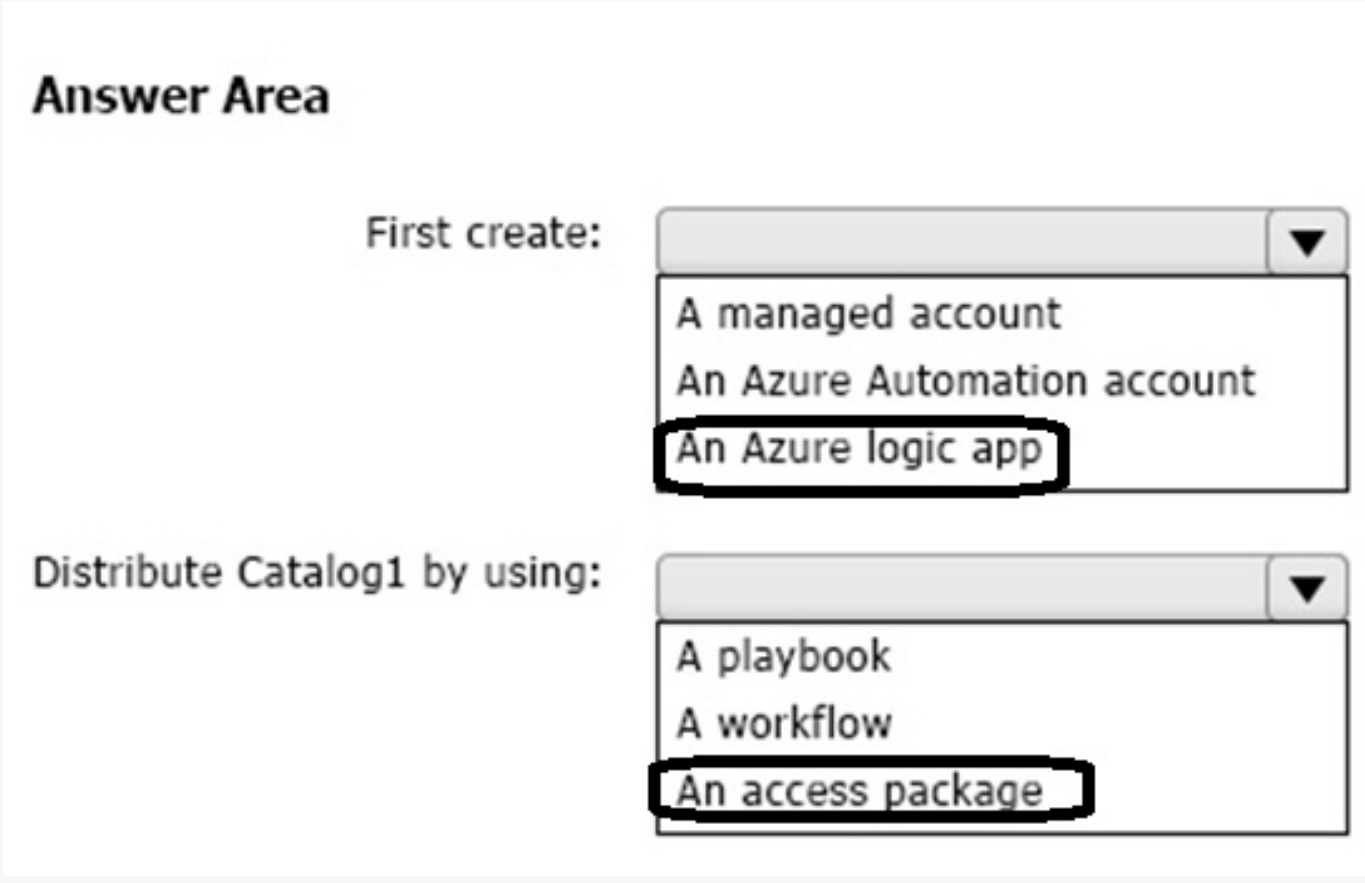
First create:

- A managed account
- An Azure Automation account
- An Azure logic app

Distribute Catalog1 by using:

- A playbook
- A workflow
- An access package

Answer:



Question: 142

CertyIQ

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

Answer: B

Explanation:

Correct answer.Basically, some administrative roles, by design can only use strong, two-gate password reset policy, regardles of SSPR settings. User Administrator and Password Administrator will be always forced to use two methods and cannot use security questions. Securiry Reader and User will use whatever is set under SSPR, so security questions in this case.

https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-policy#administrator-reset-policy-differences

Question: 143 CertyIQ

You have an Azure AD tenant.

You need to implement smart lockout with a lockout threshold of 10 failed sign-ins.

What should you configure in the Azure AD admin center?

A.Authentication strengths
B.Password protection
C.User risk policy
D.Sign-in risk policy

Answer: B

Explanation:

Correct answer is B:Password protection.

Question: 144 CertyIQ

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.

Answer: A

Explanation:

Disable Security defaults is a correct answer.

Question: 145 CertyIQ

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

Answer: D

Explanation:

The Azure AD Password Protection proxy service.

Reference:

https://learn.microsoft.com/en-us/entra/identity/authentication/concept-password-ban-bad-on-premises#how-microsoft-entra-password-protection-works

Question: 146 CertyIQ

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

Answer: D

Explanation:

a verification code from the Microsoft Authenticator app.

Question: 147 CertyIQ

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

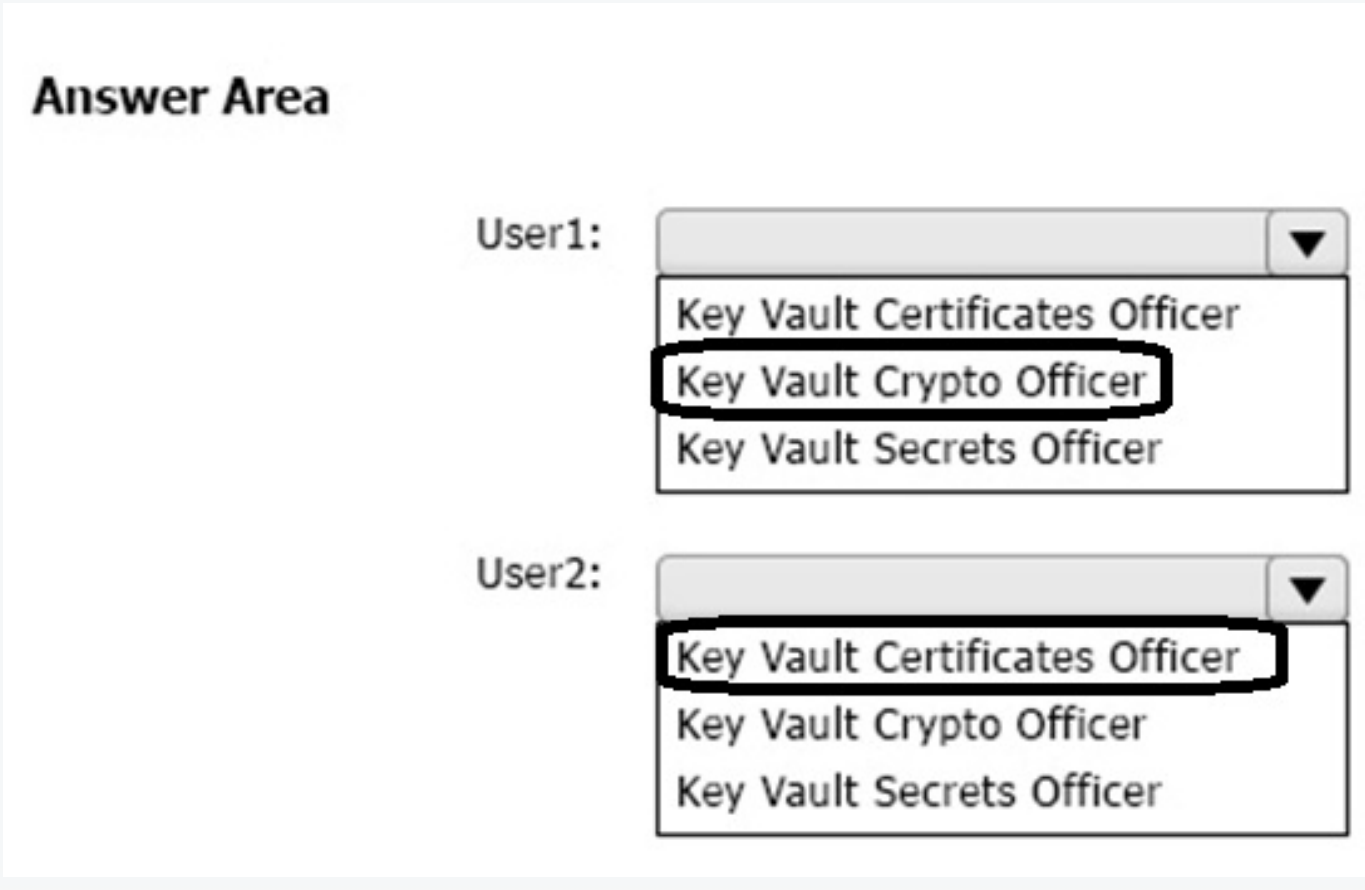
You need to configure access to Vault1. The solution must meet the following requirements:

•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:



Question: 148 CertyIQ

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

Answer: AE

Explanation:
1. 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.

Question: 149

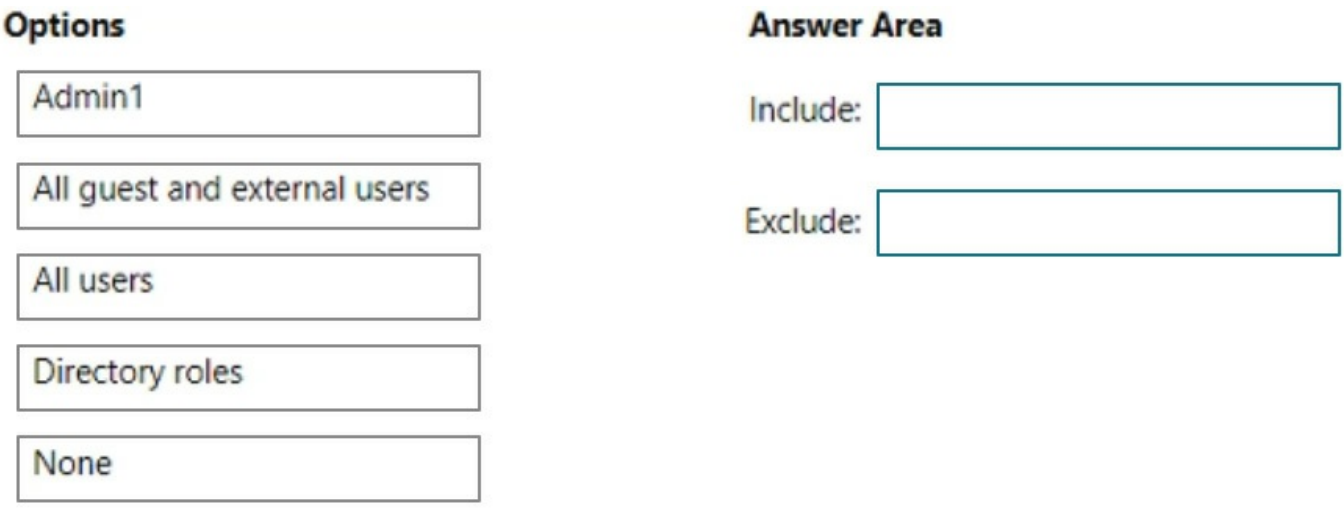
DRAG DROP
-

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



Answer:

Answer Area

Include: All users

Exclude: None

Question: 150 CertyIQ

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

Answer: B

Explanation:

B. Windows Hello for Business. It's the only option when no internet connectivity or access to a mobile phone device.

Question: 151 CertyIQ

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

Answer: A

Explanation:

a conditional access policy in Azure AD.

Question: 152 CertyIQ

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

Answer: A

Explanation:

Correct answer is A:Microsoft Authenticator.

Reference:

https://learn.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-azure-mfa

Question: 153 CertyIQ

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

oUsers or workload identities: Group1
oCloud apps or actions: Office 365 SharePoint Online
oConditions
Filter for devices: Exclude filtered devices from the policy
Rule syntax: device.displayName -startsWith “Device”
oAccess controls
Grant: Block access
Session: 0 controls selected
oEnable policy: On

•Name: CAPolicy2
•Assignments
oUsers or workload identities: Group2
oCloud apps or actions: Office 365 SharePoint Online
oConditions: 0 conditions selected
•Access controls
oGrant: Grant access
Require multifactor authentication
oSession: 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.	○	○
User2 can access Site1 from Device2.	○	○
User3 can access Site1 from Device3.	○	○

Answer:

Statements	Yes	No
User1 can access Site1 from Device1.	○	○
User2 can access Site1 from Device2.	○	○
User3 can access Site1 from Device3.	○	○

Explanation:

yes

yes

yes

Question: 154 CertyIQ

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
oUsers and groups: User1, User2, User3
oCloud apps or actions: SharePoint - Site1
•Access controls
oSession: 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

Answer: B

Explanation:

Correct answer is B:User2 only.

Question: 155 CertyIQ

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.

Answer: B

Explanation:

The correct answer is B. Delete CAPolicy1.To enable Security defaults for contoso.com, Admin1 must be assigned at least the Security Administrator role1. However, this role is not available in the list of roles for Au1, which is the only authentication method for contoso.com. This is because Au1 has a Conditional Access policy named CAPolicy1 that blocks legacy authentication protocols2. Security defaults also block legacy authentication protocols, so they cannot be enabled if there is an existing Conditional Access policy that does the same3.Therefore, to enable Security defaults, Admin1 must first delete CAPolicy1 from Au1. This will allow Admin1 to sign in to contoso.com using a legacy authentication protocol and then assign themselves the Security Administrator role. After that, Admin1 can enable Security defaults for contoso.com.

Question: 156 CertyIQ

DRAG DROP
-

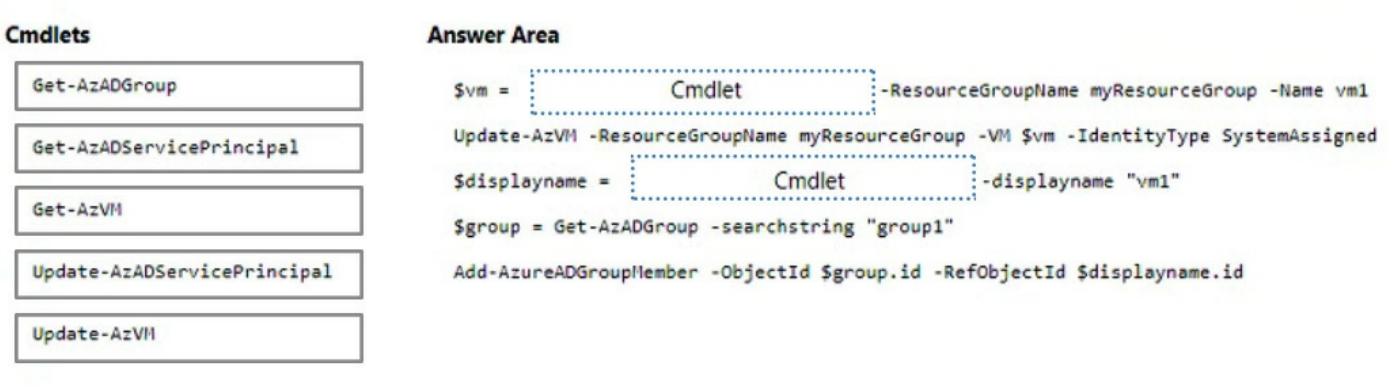
You have an Azure subscription that is linked to an Azure AD tenant named contoso.com. The subscription contains a group named Group1 and a virtual machine named VM1.

You need to meet the following requirements:

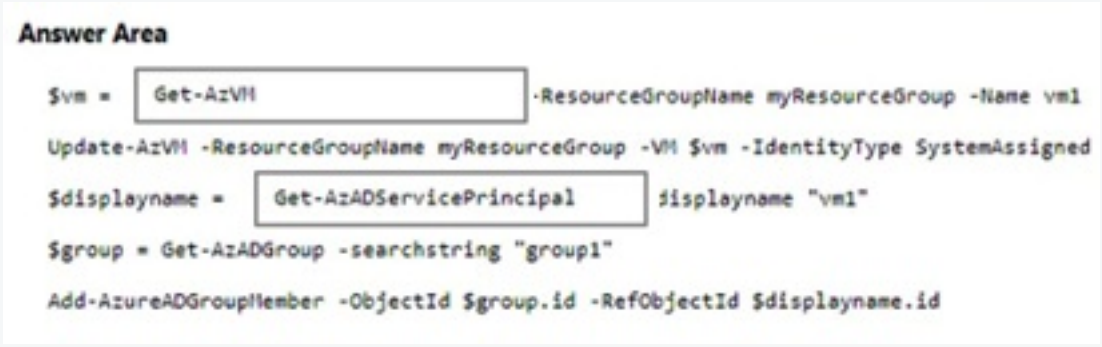
•Enable a system-assigned managed identity for VM1.
•Add VM1 to Group1.

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.



Answer:



Question: 157 CertyIQ

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.

Answer: A

Explanation:

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.

Question: 158 CertyIQ

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

Answer: B

Explanation:

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

Question: 159 CertyIQ

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

Answer: A

Explanation:

Correct answer is A:an access package.

Question: 160 CertyIQ

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

Answer: A

Explanation:

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.

Question: 161 CertyIQ

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:
oInclude: Group1
oExclude: Group2
•Sign-in risk: Medium and above
•Access controls:
oGrant 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.	○	○
User2 must change their password during sign in.	○	○
User3 must change their password during sign in.	○	○

Answer:

Answer Area

Statements	Yes	No
User1 must change their password during sign in.	●	○
User2 must change their password during sign in.	○	●
User3 must change their password during sign in.	○	●

Question: 162 CertyIQ

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

Answer: C

Explanation:

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.

Question: 163 CertyIQ

HOTSPOT -
You have a Microsoft 365 tenant and an Active Directory domain named adatum.com.
You deploy Azure AD Connect by using the Express Settings.
You need to configure self-service password reset (SSPR) to meet the following requirements:
- When users reset their password, they must be prompted to respond to a mobile app notification or answer three predefined security questions.
- Passwords must be synced between the tenant and the domain regardless of where the password was reset.

What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

From the Password reset blade in the Azure Active Directory admin center, configure:
- Authentication methods
- Notifications
- Properties
- Registration

From Azure AD Connect, enable:
- Federation with Active Directory Federation Services (AD FS)
- Pass-through authentication
- Password hash synchronization
- Password writeback

Answer:

Answer Area

From the Password reset blade in the Azure Active Directory admin center, configure:
- Authentication methods
- Notifications
- Properties
- Registration

From Azure AD Connect, enable:
- Federation with Active Directory Federation Services (AD FS)
- Pass-through authentication
- Password hash synchronization
- Password writeback

Explanation:

1) You have Go to Azure active directory > under Manage section Password reset blade > Authentication methods & check the Security Questions

2) Inorder to sync password between Domain & tenant either you have to do password hash sync & Pass through authentication with password writeback enable in Azure Ad Connect.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-security-questions

Question: 164 CertyIQ

HOTSPOT -
You have a Microsoft 365 tenant.
Sometimes, users use external, third-party applications that require limited access to the Microsoft 365 data of the respective user. The users register the applications in Azure Active Directory (Azure AD).
You need to receive an alert if a registered application gains read and write access to the users' email.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

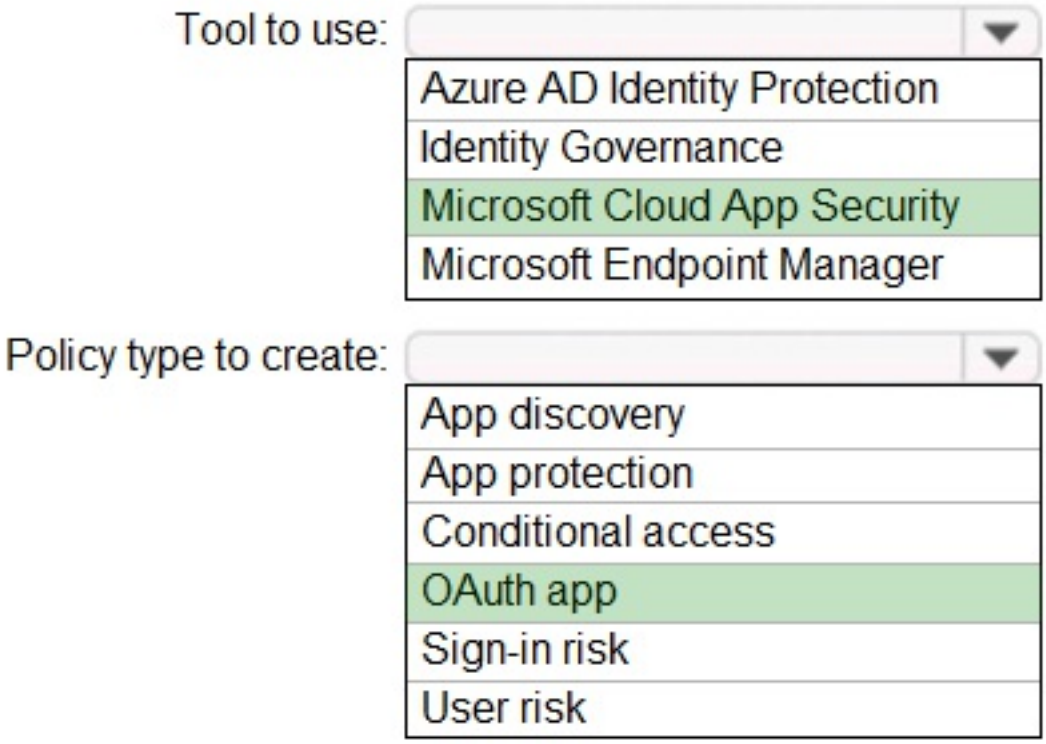
Answer Area

Tool to use:
- Azure AD Identity Protection
- Identity Governance
- Microsoft Cloud App Security
- Microsoft Endpoint Manager

Policy type to create:
- App discovery
- App protection
- Conditional access
- OAuth app
- Sign-in risk
- User risk

Answer:

Answer Area



Explanation:

Microsoft Cloud App Security. It's now called Microsoft Defender for Cloud Apps

you can set permission policies so that you get automated notifications when an OAuth app meets certain criteria.

Malicious OAuth app consent Scans OAuth apps connected to your environment and triggers an alert when a potentially malicious app is authorized.

Reference:

https://docs.microsoft.com/en-us/cloud-app-security/app-permission-policy

Question: 165 CertyIQ

You have a Microsoft 365 tenant.
The Azure Active Directory (Azure AD) tenant syncs to an on-premises Active Directory domain.
Users connect to the internet by using a hardware firewall at your company. The users authenticate to the firewall by using their Active Directory credentials.
You plan to manage access to external applications by using Azure AD.
You need to use the firewall logs to create a list of unmanaged external applications and the users who access them.
What should you use to gather the information?

A. Application Insights in Azure Monitor
B. access reviews in Azure AD
C. Cloud App Discovery in Microsoft Cloud App Security
D. enterprise applications in Azure AD

Answer: C

Explanation:

Reference:
https://docs.microsoft.com/en-us/cloud-app-security/create-snapshot-cloud-discovery-reports#using-traffic-logs-for-cloud-discovery

Question: 166 CertyIQ

HOTSPOT -
You have an on-premises datacenter that contains the hosts shown in the following table.

Name	Description
Server1	Domain controller that runs Windows Server 2019
Server2	Server that runs Windows Server 2019 and has Azure AD Connect deployed
Server3	Server that runs Windows Server 2019 and has a Microsoft ASP.NET application named App1 installed
Server4	Unassigned server that runs Windows Server 2019
Firewall1	Hardware firewall connected to the internet that blocks all traffic unless explicitly allowed

The Active Directory forest syncs to an Azure Active Directory (Azure AD) tenant. Multi-factor authentication (MFA) is enforced for Azure AD.
You need to ensure that you can publish App1 to Azure AD users.
What should you configure on Server4 and Firewall1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

Service to install on Server4:

- Azure AD Application Proxy
- The Azure AD Password Protection DC agent
- The Azure AD Password Protection proxy service
- Web Application Proxy in Windows Server

Rule to configure on Firewall1:

- Allow incoming HTTPS connections from Azure AD to Server4.
- Allow incoming IPsec connections from Azure AD to Server4.
- Allow outbound HTTPS connections from Server4 to Azure AD.
- Allow outbound IPsec connections from Server4 to Azure AD.

Answer:

Answer Area

Service to install on Server4:

- Azure AD Application Proxy
- The Azure AD Password Protection DC agent
- The Azure AD Password Protection proxy service
- Web Application Proxy in Windows Server

Rule to configure on Firewall1:

- Allow incoming HTTPS connections from Azure AD to Server4.
- Allow incoming IPsec connections from Azure AD to Server4.
- Allow outbound HTTPS connections from Server4 to Azure AD.
- Allow outbound IPsec connections from Server4 to Azure AD.

Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-proxy

Question: 167 CertyIQ

HOTSPOT -
You have an Azure Active Directory (Azure AD) tenant that has the default App registrations settings. The tenant contains the users shown in the following table.

Name	Role
Admin1	Application administrator
Admin2	Application developer
Admin3	Cloud application administrator
User1	User

You purchase two cloud apps named App1 and App2. The global administrator registers App1 in Azure AD.
You need to identify who can assign users to App1, and who can register App2 in Azure AD.
What should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

Can assign users to App1:

- Admin1 only
- Admin3 only
- Admin1 and Admin3 only
- Admin1, Admin2, and Admin3 only
- Admin1, Admin2, Admin3, and User1

Can register App2 in Azure AD:

- Admin1 only
- Admin3 only
- Admin1 and Admin3 only
- Admin1, Admin2, and Admin3 only
- Admin1, Admin2, Admin3, and User1

Answer:

Answer Area

Can assign users to App1:

- Admin1 only
- Admin3 only
- **Admin1 and Admin3 only**
- Admin1, Admin2, and Admin3 only
- Admin1, Admin2, Admin3, and User1

Can register App2 in Azure AD:

- Admin1 only
- Admin3 only
- Admin1 and Admin3 only
- Admin1, Admin2, and Admin3 only
- **Admin1, Admin2, Admin3, and User1**

Explanation:

Only administrators (Admin1 - Application Administrator & Admin3 - Cloud application administrator) can manage/configure apps.

Name: Cloud application administrator

Description: Users in this role can add, manage, and configure enterprise applications, app registrations but will not be able to configure or manage on-premises like app proxy.

Azure AD - User settings - App registration: default is Yes (If this option is set to yes, then non-admin users may register custom-developed applications for use within this directory.)

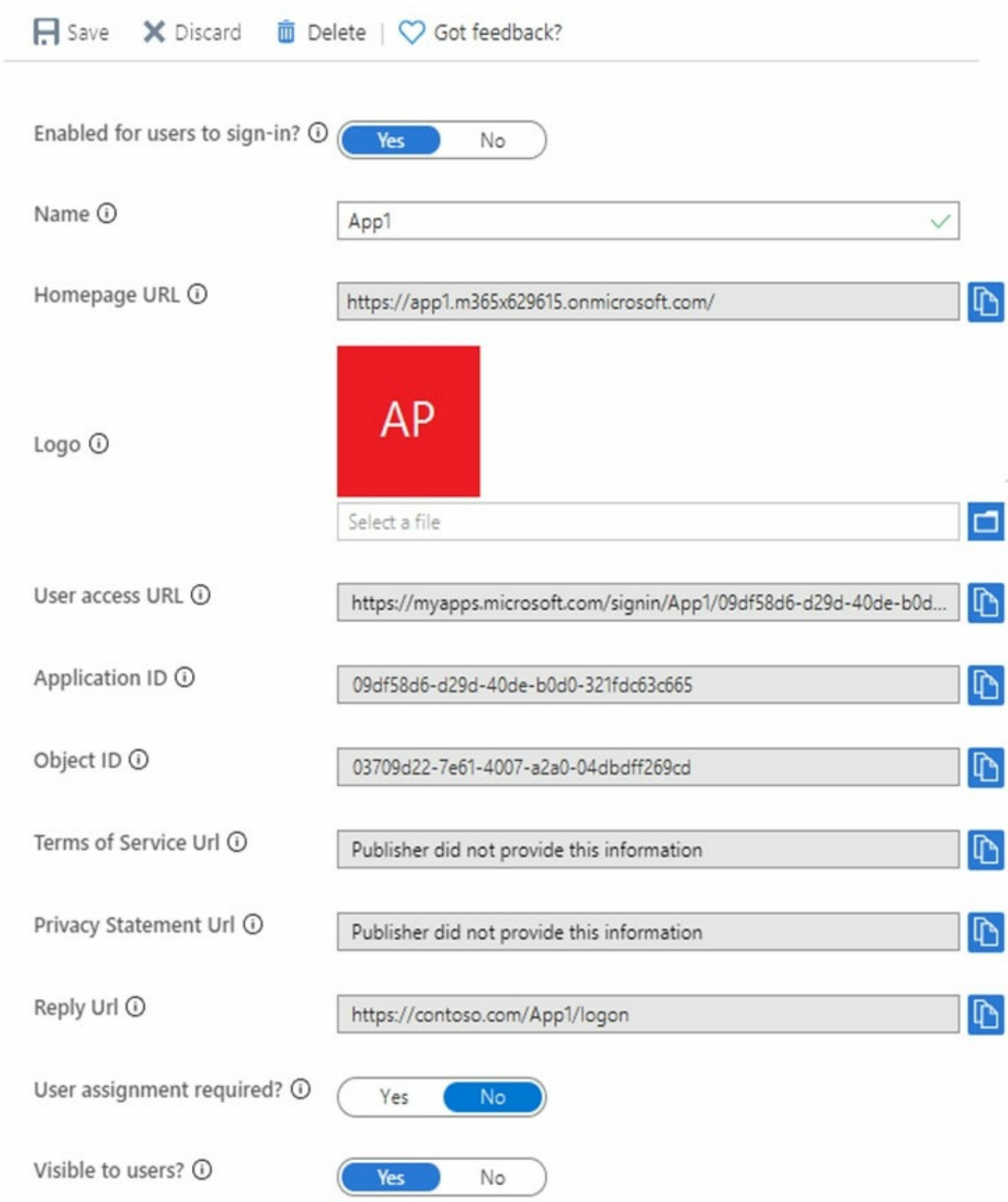
Reference:

https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/add-application-portal-assign-users
https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added

Question: 168

CertyIQ

HOTSPOT -
You have a custom cloud app named App1 that is registered in Azure Active Directory (Azure AD).
App1 is configured as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

[answer choice] can access App1 from the homepage URL.

- All users
- No one
- Only users listed on the Owners blade
- Only users listed on the Users and groups blade

App1 will appear in the Microsoft Office 365 app launcher for **[answer choice]**.

- all users
- no one
- only users listed on the Owners blade
- only users listed on the Users and groups blade

Answer:

Answer Area

[answer choice] can access App1 from the homepage URL.

- All users
- No one
- Only users listed on the Owners blade
- Only users listed on the Users and groups blade

App1 will appear in the Microsoft Office 365 app launcher for **[answer choice]**.

- all users
- no one
- only users listed on the Owners blade
- only users listed on the Users and groups blade

Explanation:

1)The valid Answer is All user can access app by using hompage url.

2) only assigned users and group will able to access through myapps.microsoft.com

so the answer is 1 & 4

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/add-application-portal-configure

https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal

Question: 169

You have an Azure Active Directory (Azure AD) tenant.
You create an enterprise application collection named HR Apps that has the following settings:
- Applications: App1, App2, App3
- Owners: Admin1
- Users and groups: HRUsers

All three apps have the following Properties settings:
- Enabled for users to sign in: Yes
- User assignment required: Yes

Visible to users: Yes -

Users report that when they go to the My Apps portal, they only see App1 and App2.
You need to ensure that the users can also see App3.
What should you do from App3?

A. From Users and groups, add HRUsers.
B. From Single sign-on, configure a sign-on method.
C. From Properties, change User assignment required to No.
D. From Permissions, review the User consent permissions.

Answer: A

Explanation:

Correct Answer. A

I just tried this in my company's tenancy. User assignment and Visible to Users goes hand in hand for this.

If Visible to Users is set to Yes then this is the explanation from the 'i' next to it:

If this option is set to yes, then assigned users will see the application on My Apps and O365 app launcher. If this option is set to no, then no users will see this application on their My Apps and O365 launcher. Assigned User is the key here.

Unless the users are assigned to the app, then No one will see the application on their MyApps or O365 Launcher. Provided Answer is Correct!

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal
https://docs.microsoft.com/en-us/azure/active-directory/user-help/my-applications-portal-workspaces

Question: 170 CertyIQ

You have an Azure Active Directory (Azure AD) tenant.
For the tenant, Users can register applications is set to No.
A user named Admin1 must deploy a new cloud app named App1.
You need to ensure that Admin1 can register App1 in Azure AD. The solution must use the principle of least privilege.
Which role should you assign to Admin1?

A. Managed Application Contributor for Subscription1.
B. Application developer in Azure AD.
C. Cloud application administrator in Azure AD.
D. App Configuration Data Owner for Subscription1.

Answer: B

Explanation:

Name: Application developer

Description: Users in this role will continue to be able to register app registrations even if the Global Admin has turned off the tenant level switch for "Users can register apps".

Application Developer Can create application registrations independent of the 'Users can register applications' setting.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

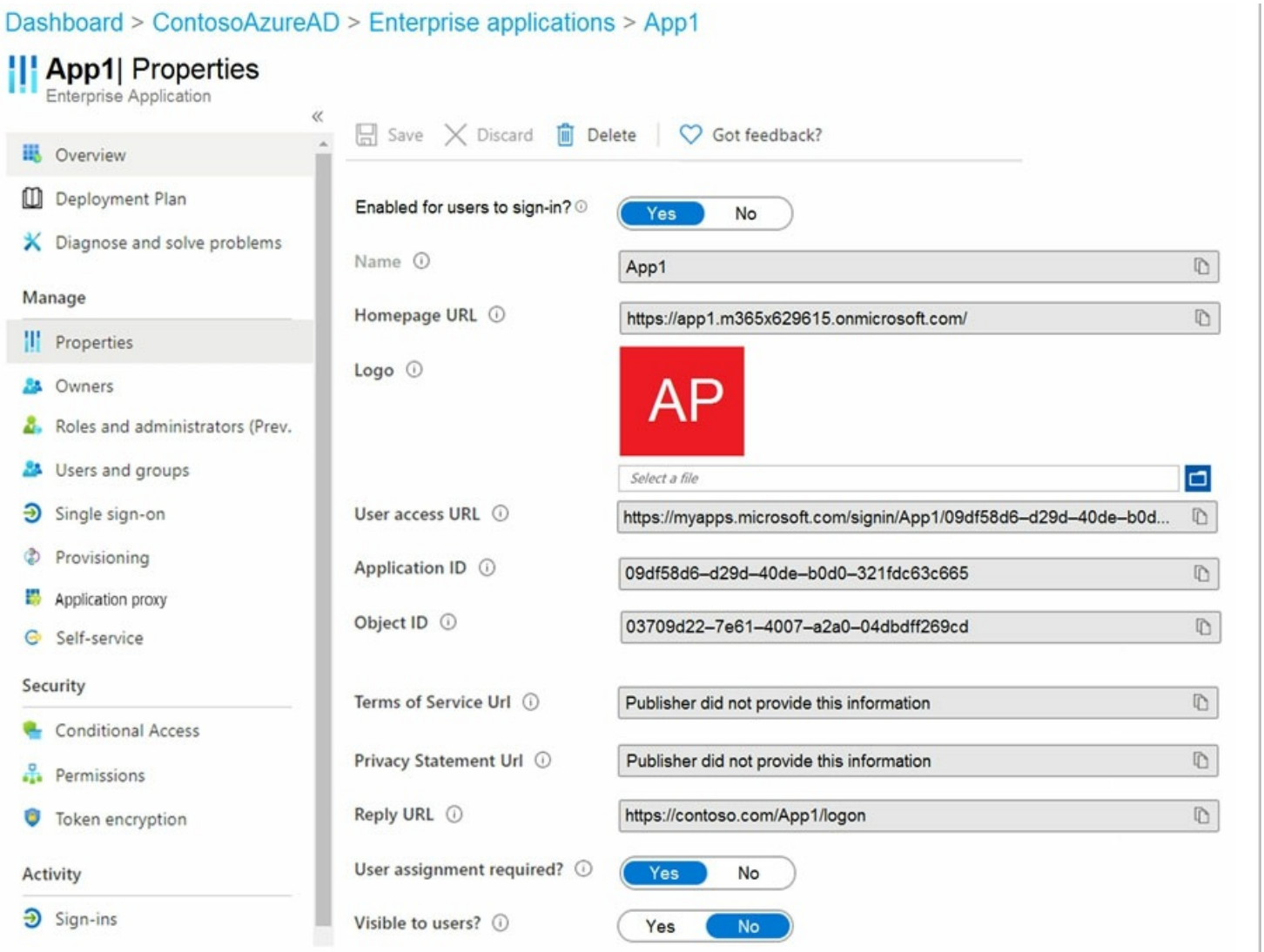
https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-app-roles

Question: 171 CertyIQ

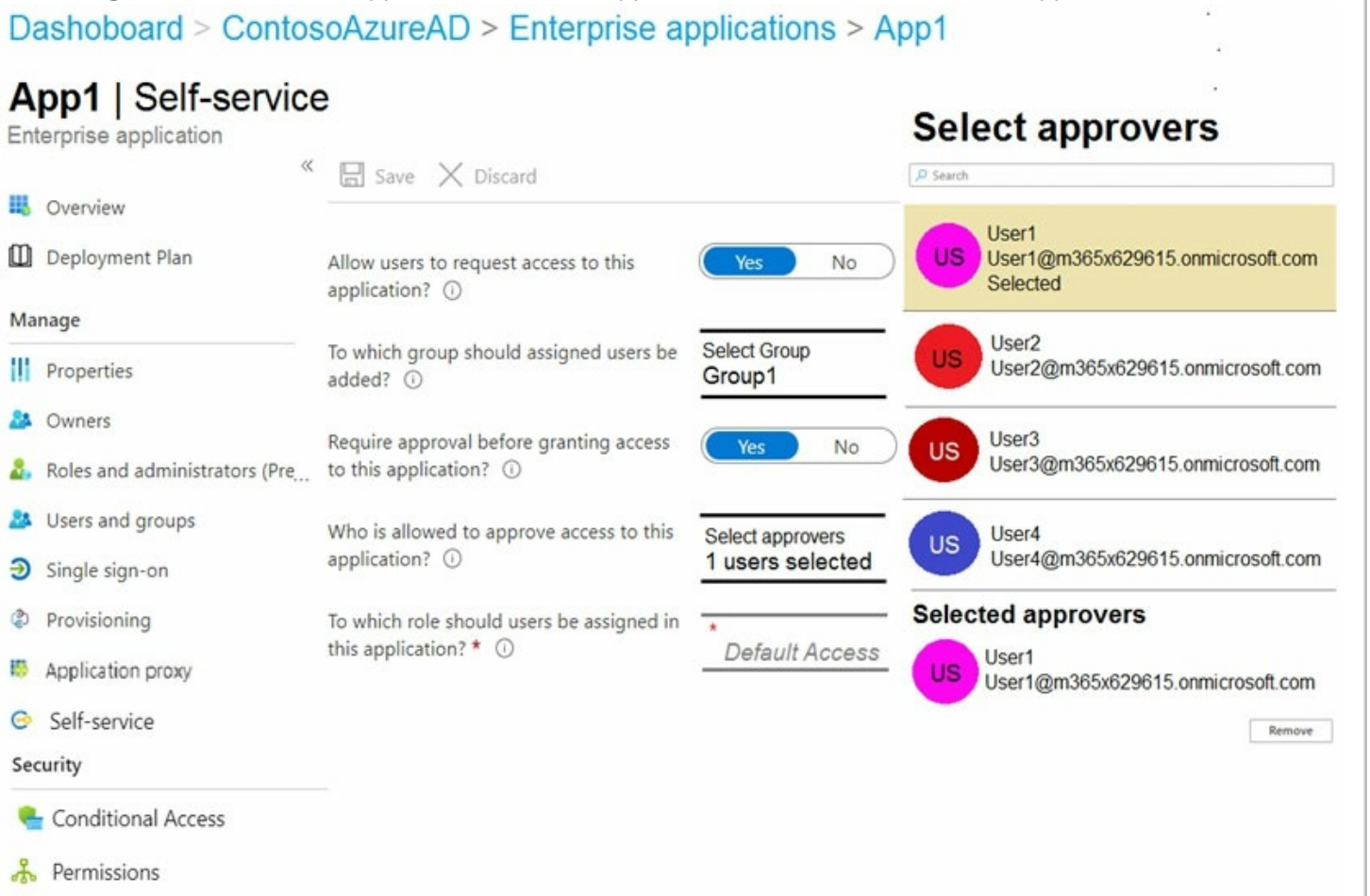
HOTSPOT -
You have a Microsoft 365 tenant that contains a group named Group1 as shown in the Group1 exhibit. (Click the Group1 tab.)

```
PS C:\> Get-AzureADGroup -searchstring "group1" | Get-AzureADGroupowner

ObjectId                             DisplayName   UserPrincipalName                UserType
--------                             -----------   -----------------                --------
a7f7d405-636f-4493-b971-5c2b7a131b1c Admin         admin@M365x629615.onmicrosoft.com Member

PS C:\> Get-AzureADGroup -searchstring "group1" | GetAzureADGroupMember | ft displayname

DisplayName
-----------
User1
User4
Group3
```

You create an enterprise application named App1 as shown in the App1 Properties exhibit. (Click the App1 Properties tab.)



You configure self-service for App1 as shown in the App1 Self-service exhibit. (Click the App1 Self-service tab.)



For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
The members of Group3 can access App1 without first being approved by User1.	○	○
After you configure self-service for App1, the owner of Group1 is User1.	○	○
App1 appears in the Microsoft Office 365 app launcher of User4.	○	○

Answer:

Answer Area

Statements	Yes	No
The members of Group3 can access App1 without first being approved by User1.	○	○
After you configure self-service for App1, the owner of Group1 is User1.	○	○
App1 appears in the Microsoft Office 365 app launcher of User4.	○	○

Explanation:

1. NO - Only direct members will have access. Approved users will be added to Group 1.

2. Yes - The approver will automatically become owner of the Group 1 after self service is configured.

3. NO - Visible to users is NO. So no one will be able to see the app.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/add-application-portal-assign-users

Question: 172 CertyIQ

You have an Azure Active Directory (Azure AD) tenant named contoso.com that has Azure AD Identity Protection enabled.
You need to implement a sign-in risk remediation policy without blocking user access.
What should you do first?

A. Configure access reviews in Azure AD.
B. Enforce Azure AD Password Protection.
C. Configure self-service password reset (SSPR) for all users.
D. Implement multi-factor authentication (MFA) for all users.

Answer: D

Explanation:

MFA and SSPR are both required. However, MFA is required first.

to implement a sign-in risk remediation policy

When a sign in risk policy triggers:

Azure AD MFA can be triggered, allowing to user to prove it's them by using one of their registered authentication methods, resetting the sign in risk.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-remediate-unblock https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment

Question: 173 CertyIQ

HOTSPOT -
Your company has a Microsoft 365 tenant.
All users have computers that run Windows 10 and are joined to the Azure Active Directory (Azure AD) tenant.
The company subscribes to a third-party cloud service named Service1. Service1 supports Azure AD authentication and authorization based on OAuth. Service1 is published to the Azure AD gallery.
You need to recommend a solution to ensure that the users can connect to Service1 without being prompted for authentication. The solution must ensure that the users can access Service1 only from Azure AD-joined computers.
The solution must minimize administrative effort.
What should you recommend for each requirement? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

Ensure that the users can connect to Service1 without being prompted for authentication:

- An app registration in Azure AD
- Azure AD Application Proxy
- An enterprise application in Azure AD
- A managed identity in Azure AD

Ensure that the users can access Service1 only from the Azure AD-joined computers:

- Azure AD Application Proxy
- A compliance policy
- A conditional access policy
- An OAuth policy

Answer:

Answer Area

Ensure that the users can connect to Service1 without being prompted for authentication:

- An app registration in Azure AD
- Azure AD Application Proxy
- An enterprise application in Azure AD
- A managed identity in Azure AD

Ensure that the users can access Service1 only from the Azure AD-joined computers:

- Azure AD Application Proxy
- A compliance policy
- A conditional access policy
- An OAuth policy

Explanation:

Service1 support OAuth for Authentication & authorization, however service1 is published in Azure AD gallery, hence we will use An enterprise application in Azure AD blade to register for SSO.

for second point, we can use conditional Access policy to restrict.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/require-managed-devices

Question: 174

Your company requires that users request access before they can access corporate applications.
You register a new enterprise application named MyApp1 in Azure Active Directory (Azure AD) and configure single sign-on (SSO) for MyApp1.
Which settings should you configure next for MyApp1?

A. Self-service
B. Provisioning
C. Application proxy
D. Roles and administrators

Answer: A

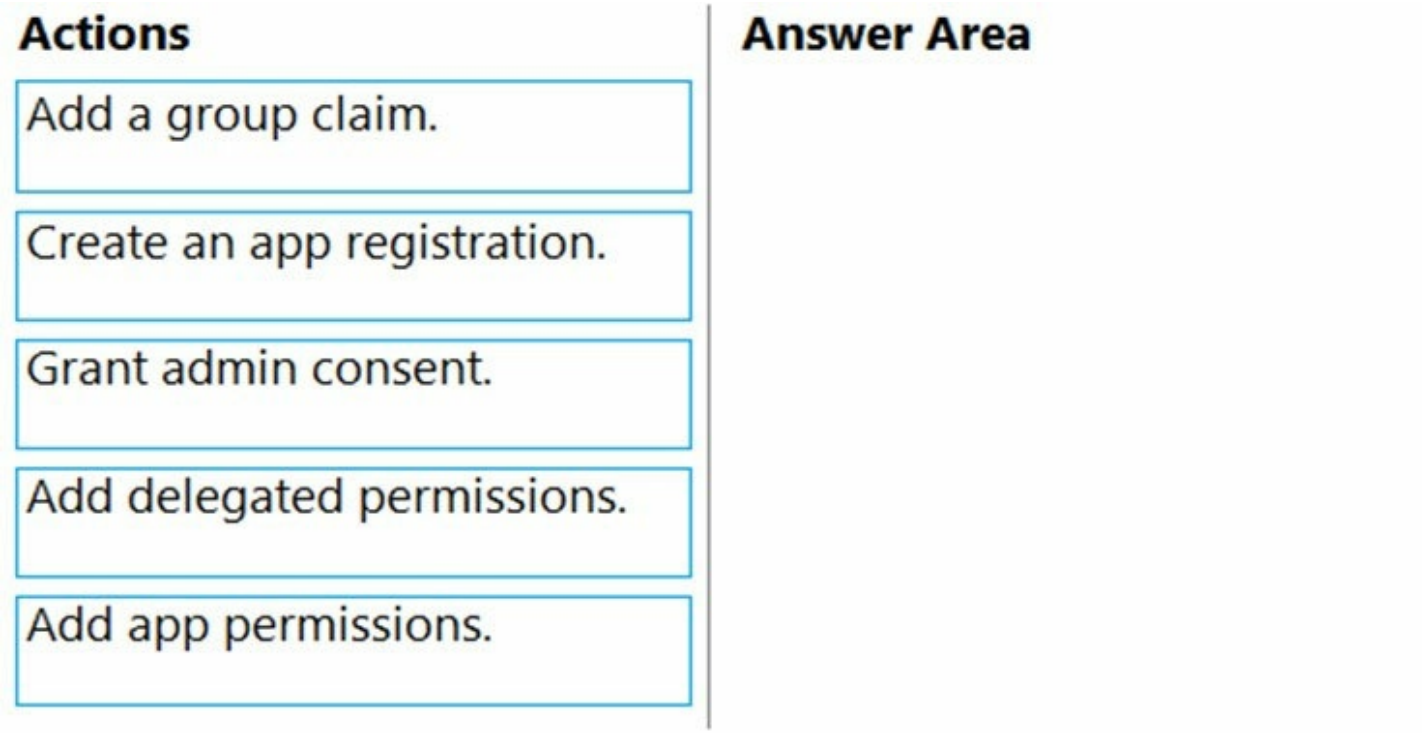
Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/manage-self-service-access

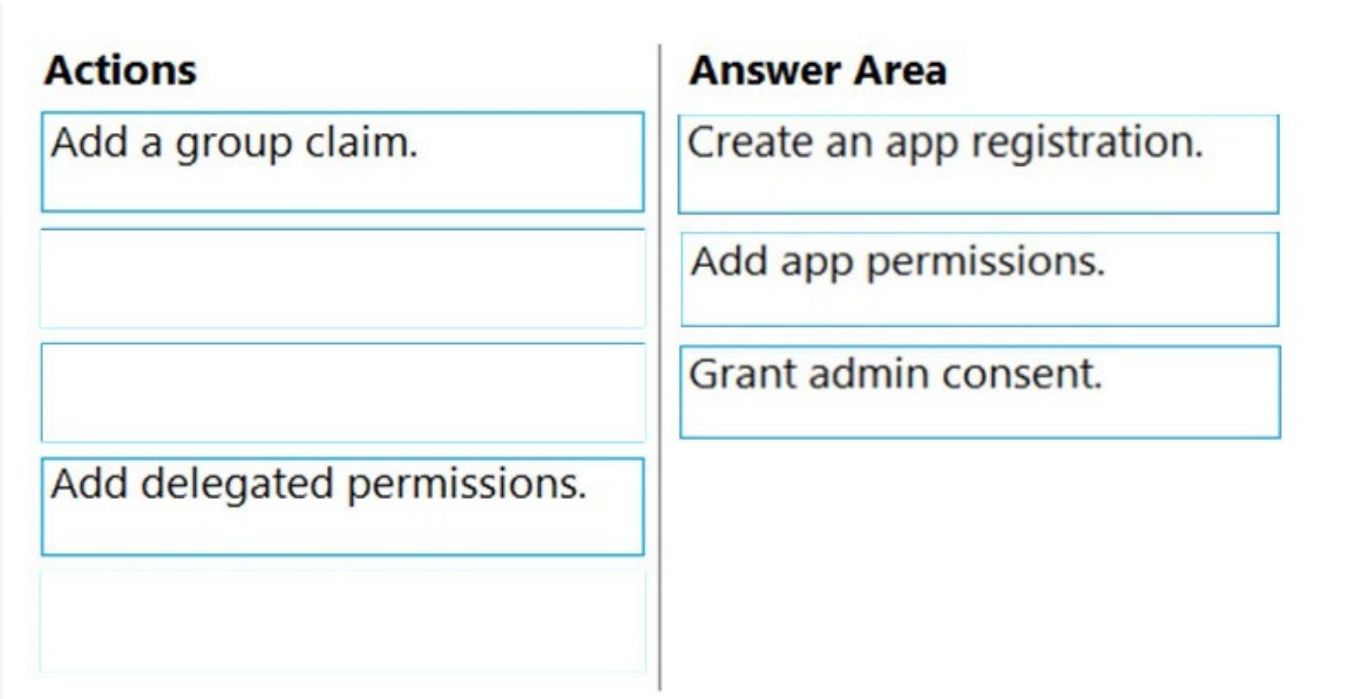
Question: 175

CertyIQ

DRAG DROP -
Your company has an Azure Active Directory (Azure AD) tenant named contoso.com.
The company is developing a web service named App1.
You need to ensure that App1 can use Microsoft Graph to read directory data in contoso.com.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange then in the correct order.
Select and Place:



Answer:



Explanation:

First, we need to register a new application

Then we need to add application permissions

And then we need to grant admin consent

Reference:

https://docs.microsoft.com/en-us/graph/auth/auth-concepts

Question: 176 CertyIQ

You have an Azure Active Directory (Azure AD) tenant that contains cloud-based enterprise apps.
You need to group related apps into categories in the My Apps portal.
What should you create?

A. tags
B. collections
C. naming policies
D. dynamic groups

Answer: B

Explanation:

In the My Apps portal, applications appear in default collections and your custom app collections. The Apps collection in My Apps is a default collection that contains all the applications that have been assigned to you, sorted alphabetically.

B is the correct answer based on the link provided.

Reference:

https://support.microsoft.com/en-us/account-billing/customize-app-collections-in-the-my-apps-portal-2dae6b8a-d8b0-4a16-9a5d-71ed4d6a6c1d

Question: 177 CertyIQ

The Azure Active Directory (Azure AD) tenant contains the groups shown in the following table.

Name	Type
Group1	Security
Group2	Distribution
Group3	Microsoft 365
Group4	Mail-enabled security

In Azure AD, you add a new enterprise application named App1.
Which groups can you assign to App1?

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

Answer: D

Explanation:

- Group-based assignment is supported for Security groups only.

- Nested group memberships and Microsoft 365 groups aren't currently supported.

https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal?pivots=portal

Question: 178 CertyIQ

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

Name	Role
User1	None
User2	None
Admin1	Application administrator
Admin2	Authentication administrator

The User settings for enterprise applications have the following configurations:
- Users can consent to apps accessing company data on their behalf: No
- Users can consent to apps accessing company data for the groups they own: No
- Users can request admin consent to apps they are unable to consent to: Yes

Who can review admin consent requests: Admin2, User2

User1 attempts, to add an app that requires consent to access company data.
Which user can provide consent?

A. User1
B. User2
C. Admin1
D. Admin2

Answer: C

Explanation:
To approve requests, a reviewer must be a global administrator, cloud application administrator, or application administrator.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/configure-admin-consent-workflow

Question: 179 CertyIQ

You have a Microsoft 365 subscription. The subscription contains users that use Microsoft Outlook 2016 and Outlook 2013 clients.
You need to implement tenant restrictions. The solution must minimize administrative effort.
What should you do first?

A. Configure the Outlook 2013 clients to use modern authentication.
B. Upgrade the Outlook 2013 clients to Outlook 2016.
C. From the Exchange admin center, configure Organization Sharing.
D. Upgrade all the Outlook clients to Outlook 2019.

Answer: A

Explanation:

Microsoft Office 2013 on Microsoft Windows computers supports Modern authentication. But, to turn it on, you need to configure the following registry keys

https://learn.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/enable-modern-authentication?view=o365-worldwide

Question: 180 CertyIQ

You have a Microsoft 365 E5 subscription.

You need to create a Microsoft Defender for Cloud Apps session policy.

What should you do first?

A. From the Microsoft Defender for Cloud Apps portal, select User monitoring.
B. From the Microsoft Defender for Cloud Apps portal, select App onboarding/maintenance.

C. From the Azure Active Directory admin center, create a Conditional Access policy.

D. From the Microsoft Defender for Cloud Apps portal, create a continuous report.

Answer: C

Explanation:

what I should do first is:

From the Azure Active Directory admin center, create a Conditional Access policy.

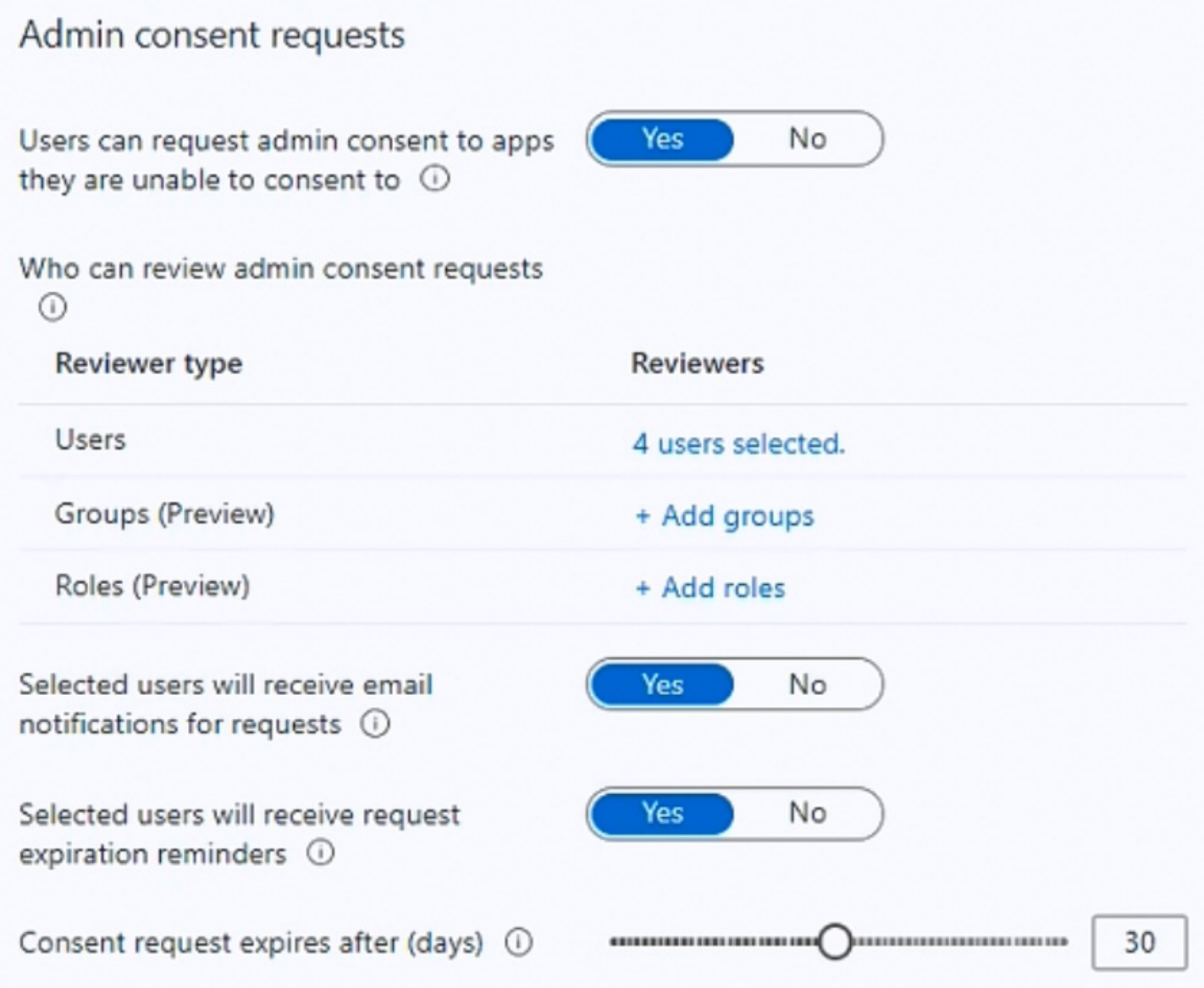
Question: 181 CertyIQ

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

Name	Role
Admin1	Cloud application administrator
Admin2	Application administrator
Admin3	Security administrator
User1	None

You add an enterprise application named App1 to Azure AD and set User1 as the owner of App1. App1 requires admin consent to access Azure AD before the app can be used.

You configure the Admin consent requests settings as shown in the following exhibit.



Admin1, Admin2, Admin3, and User' are added as reviewers.

Which users can review and approve the admin consent requests?

A. Admin1 only
B. Admin1, Admin2 and Admin3 only
C. Admin1, Admin2, and User1 only
D. Admin1 and Admin2 only
E. Admin1, Admin2, Admin3, and User1

Answer: D

Explanation:

https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/configure-admin-consent-workflow

"To approve requests, a reviewer must be a global administrator, cloud application administrator, or application administrator. The reviewer must already have one of these admin roles assigned; simply designating them as a reviewer doesn't elevate their privileges."

Question: 182 CertyIQ

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1.

You need to be notified if a user downloads more than 50 files in one minute from Site1.

Which type of policy should you create in the Microsoft Defender for Cloud Apps portal?

A. session policy
B. activity policy
C. file policy
D. anomaly detection policy

Answer: B

Explanation:

Custom alerts in Activity policies

https://learn.microsoft.com/en-us/defender-cloud-apps/user-activity-policies

Question: 183 CertyIQ

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1. Site1 hosts PDF files.

You need to prevent users from printing the files directly from Site1.

Which type of policy should you create in the Microsoft Defender for Cloud Apps portal?

A. activity policy
B. access policy
C. file policy
D. session policy

Answer: D

Explanation:

Correct

https://learn.microsoft.com/en-us/defender-cloud-apps/session-policy-aad

Question: 184 CertyIQ

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps and Conditional Access policies.

You need to block access to cloud apps when a user is assessed as high risk.

Which type of policy should you create in the Microsoft Defender for Cloud Apps portal?

A. access policy
B. OAuth app policy
C. anomaly detection policy
D. activity policy

Answer: A

Question: 185 CertyIQ

You have a Microsoft 365 E5 subscription.

Users authorize third-party cloud apps to access their data.

You need to configure an alert that will be triggered when an app requires high permissions and is authorized by more than 20 users.

Which type of policy should you create in the Microsoft Defender for Cloud Apps portal?

A. anomaly detection policy
B. OAuth app policy
C. access policy
D. activity policy

Answer: B

Explanation:

https://learn.microsoft.com/en-us/defender-cloud-apps/app-permission-policy

In addition to the existing investigation of OAuth apps connected to your environment, you can set permission policies so that you get automated notifications when an OAuth app meets certain criteria. For example, you can automatically be alerted when there are apps that require a high permission level and were authorized by more than 50 users

Question: 186 CertyIQ

Your company has an Azure AD tenant that contains the users shown in the following table.

Name	Role
User1	Application administrator
User2	None
User3	Exchange administrator
User4	Cloud application administrator

You have the app registrations shown in the following table.

App name	Used by	Microsoft Graph permission
App1	User1	Calendars.Read of type Delegated
App2	User2	Calendars.Read of type Delegated Calendars.ReadWrite of type Application
App3	User3, User4	Calendars.Read of type Application

A company policy prevents changes to user permissions.

Which user can create appointments in the calendar of each user at the company?

A. User1
B. User2
C. User3
D. User4

Answer: B

Explanation:

User2 is the only one who has access to Application.write for the calendar.

Question: 187 CertyIQ

You have an Azure AD tenant that contains a user named User1 and a registered app named App1.

User1 deletes the app registration of App1.

You need to restore the app registration.

What is the maximum number of days you have to restore the app registration from when it was deleted?

A. 14
B. 30
C. 60
D. 180

Answer: B

Explanation:

30 is a correct answer.

Question: 188 CertyIQ

HOTSPOT
-

You have a Microsoft 365 tenant.

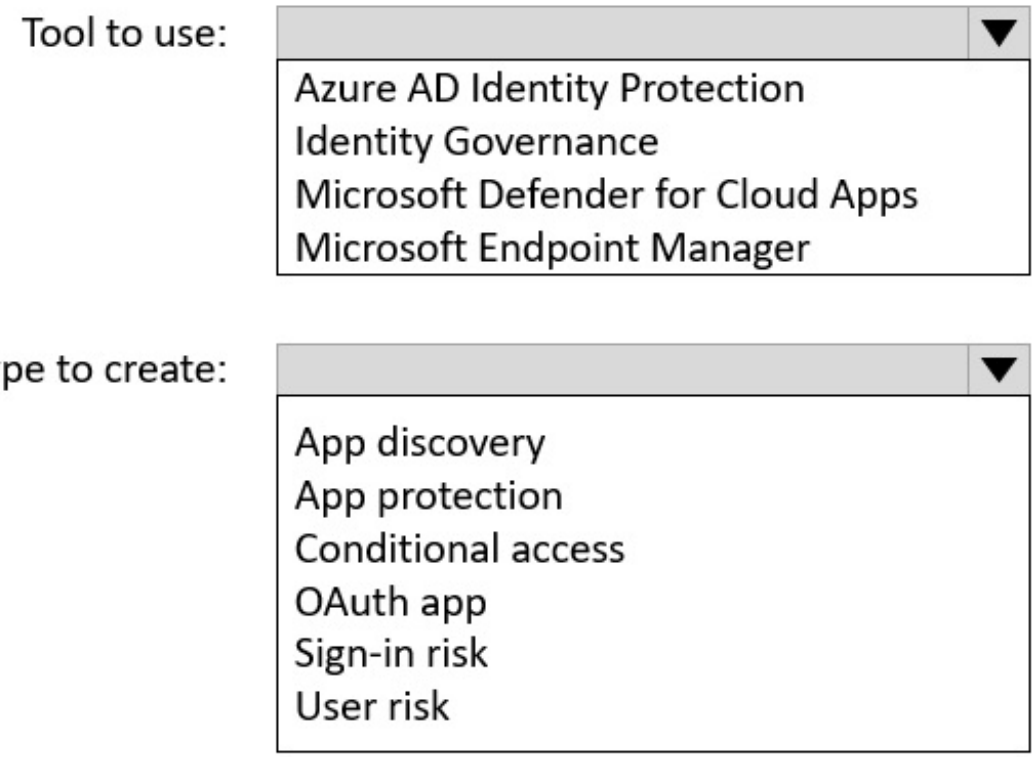
Sometimes, users use external, third-party applications that require limited access to the Microsoft 365 data of the respective user. The users register the applications in Azure AD.

You need to receive an alert if a registered application gains read and write access to the users' email.

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

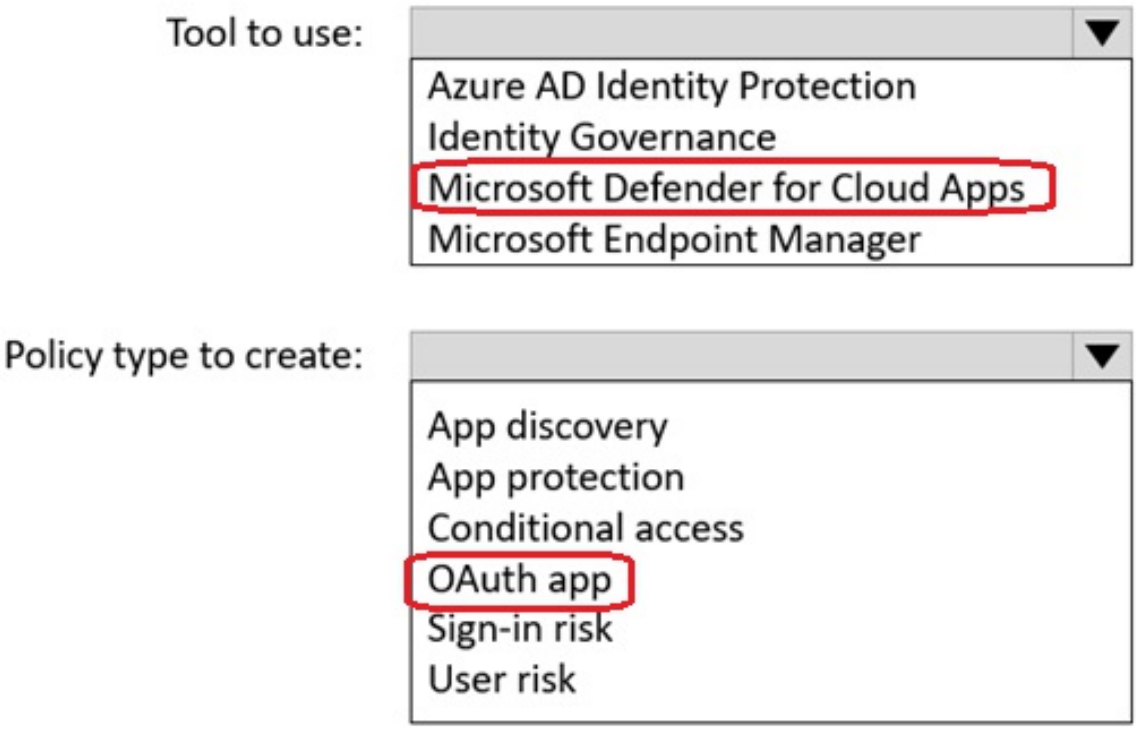
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area



Question: 189 CertyIQ

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 implement the planned changes for application access to organizational data.

What should you configure?

A.authentication methods
B.the User consent settings
C.access packages
D.an application proxy

Answer: C

Explanation:
1. Azure Portal> Azure AD > Identity Governance > (Entitlement Management Heading) Access Packages > + New Access Package (from the top bar) > (Resources tab) + Applications > (Requests tab) in the section "users who can requests" we check box " for users in your directory), and then "all members(incl. guests), and then in the section " approval, we select "Yes" ..etc

Question: 190

CertyIQ

You have an Azure AD tenant.

You configure User consent settings to allow users to provide consent to apps from verified publishers.

You need to ensure that the users can only provide consent to apps that require low impact permissions.

What should you do?

A.Create an enterprise application collection.
B.Create an access review.
C.Create an access package.
D.Configure permission classifications.

Answer: D

Explanation:
1. I go with Dhttps://learn.microsoft.com/en-us/azure/active-directory/manage-apps/configure-permission-classifications?pivots=portal

Question: 191 CertyIQ

HOTSPOT
-

You have a Microsoft 365 E5 subscription that contains a user named User1.

You configure app governance integration.

User1 needs to view the App governance dashboard. The solution must use the principle of the least privilege.

Which role should you assign to User1, and which portal should User1 use to view the dashboard? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Role:

- Application Administrator
- Application Developer
- Cloud Application Administrator

Portal:

- The Microsoft 365 admin center
- The Microsoft 365 Defender portal
- The Microsoft Defender for Cloud Apps portal
- The Microsoft Purview compliance portal

Answer:

Explanation:

https://learn.microsoft.com/en-us/defender-cloud-apps/app-governance-get-started#roles

Question: 192 CertyIQ

You have an Azure subscription.

You are evaluating enterprise software as a service (SaaS) apps.

You need to ensure that the apps support automatic provisioning of Azure AD users.

Which specification should the apps support?

A.OAuth 2.0
B.WS-Fed
C.SCIM 2.0
D.LDAP 3

Answer: C

Explanation:

Chttps://learn.microsoft.com/en-us/azure/active-directory/app-provisioning/user-provisioningor https://techcommunity.microsoft.com/t5/security-compliance-and-identity/provisioning-with-scim-getting-started/ba-p/880010

Question: 193 CertyIQ

You have an Azure AD tenant and a .NET web app named App1.

You need to register App1 for Azure AD authentication.

What should you configure for App1?

A.the executable name
B.the bundle ID
C.the package name
D.the redirect URI

Answer: D

Explanation:

Correct answer is D:the redirect URI.

Question: 194 CertyIQ

You have a Microsoft 365 tenant.

All users have mobile phones and Windows 10 laptops.

The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity. While working from the remote locations, the users connect their laptops to a wired network that has internet access.

You plan to implement multi-factor authentication (MFA).

Which MFA authentication method can the users use from the remote location?

A.a notification through the Microsoft Authenticator app
B.security questions
C.voice
D.Windows Hello for Business

Answer: D

Explanation:

Correct answer is D:Windows Hello for Business.

Question: 195 CertyIQ

You have an Azure AD tenant.

You discover that a large number of new apps were added to the tenant.

You need to implement an approval process for new enterprise applications.

What should you do?

A.From the Microsoft Defender for Cloud Apps portal, create a Cloud Discovery anomaly detection policy.
B.From the Microsoft Entra admin center, configure the Admin consent settings.
C.From the Microsoft Defender for Cloud Apps portal, configure an app connector.
D.From the Microsoft Entra admin center, configure an access review.

Answer: B

Explanation:

From the Microsoft Entra admin center, configure the Admin consent settings.

Reference:

https://practical365.com/use-azure-ad-admin-consent-requests-to-help-avoid-attacks-against-your-users/

Question: 196 CertyIQ

You have a Microsoft 365 E5 subscription.

You purchase the app governance add-on license.

You need to enable app governance integration.

Which portal should you use?

A.the Microsoft Defender for Cloud Apps portal
B.the Microsoft 365 admin center
C.Microsoft 365 Defender
D.the Azure Active Directory admin center
E.the Microsoft Purview compliance portal

Answer: C

Explanation:

Correct answer is C:Microsoft 365 Defender.

Reference:

https://learn.microsoft.com/en-us/defender-cloud-apps/app-governance-get-started#turn-on-app-governance

Question: 197 CertyIQ

Your company purchases a new Microsoft 365 E5 subscription and an app named App1.

You need to create a Microsoft Defender for Cloud Apps access policy for App1.

What should you do you first?

A.Configure a Conditional Access policy to use app-enforced restrictions.
B.Configure a Token configuration for App1.
C.Add an API permission for App1.
D.Configure a Conditional Access policy to use Conditional Access App Control.

Answer: D

Explanation:

Configure a Conditional Access policy to use Conditional Access App Control.

Reference:

https://learn.microsoft.com/en-us/defender-cloud-apps/proxy-intro-aad#how-it-works

Question: 198 CertyIQ

Case Study -

Overview -

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

Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure AD tenant named fabrikam.com.

Existing Environment. Existing Environment

The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named Contoso_Resources. The Contoso_Resources OU contains all users and computers.

The contoso.com Active Directory domain contains the relevant users shown in the following table.

Name	Office	Department
Admin1	Montreal	Helpdesk
User1	Montreal	HR
User2	Montreal	HR
User3	Montreal	HR
Admin2	London	Helpdesk
User4	London	Finance
User5	London	Sales
User6	London	Sales
Admin3	Seattle	Helpdesk
User7	Seattle	Sales
User8	Seattle	Sales
User9	Seattle	Sales

Contoso also includes a marketing department that has users in each office.

Existing Environment. Microsoft 365/Azure Environment

Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:

•Microsoft Office 365 Enterprise E5
•Enterprise Mobility + Security E5
•Windows 10 Enterprise E3
•Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso_Resources OU is synced.

Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.

User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:

•The users in the London office have the Microsoft 365 Phone System license unassigned.
•The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

Existing Environment. Problem Statements

Contoso identifies the following issues:

•Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.
•The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.
•The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.
•Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.
•When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes -

Contoso plans to implement the following changes:

•Implement self-service password reset (SSPR).
•Analyze Azure audit activity logs by using Azure Monitor.
•Simplify license allocation for new users added to the tenant.
•Collaborate with the users at Fabrikam on a joint marketing campaign.
•Configure the User administrator role to require justification and approval to activate.
•Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.
•For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

Contoso plans to acquire a company named A. Datum Corporation. One hundred new A. Datum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.

Requirements. Technical Requirements

Contoso identifies the following technical requirements:

•All users must be synced from AD DS to the contoso.com Azure AD tenant.
•App1 must have a redirect URI pointed to https://contoso.com/auth-response.
•License allocation for new users must be assigned automatically based on the location of the user.
•Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.
•Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.
•The helpdesk administrators must be able to manage licenses for only the users in their respective office.
•Users must be forced to change their password if there is a probability that the users' identity was compromised.

You need to meet the planned changes and technical requirements for App1.

What should you implement?

A.a policy set in Microsoft Intune

B.Azure AD Application Proxy

C.an app configuration policy in Microsoft Intune

D.an app registration in Azure AD

Answer: D

Explanation:

An app registration in Azure AD.

Question: 199 CertyIQ

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

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

You have an Amazon Web Services (AWS) account, a Google Workspace subscription, and a GitHub account.

You deploy an Azure subscription and enable Microsoft 365 Defender.

You need to ensure that you can monitor OAuth authentication requests by using Microsoft Defender for Cloud Apps.

Solution: From the Microsoft 365 Defender portal, you add the Google Workspace app connector.

Does this meet the goal?

A.Yes

B.No

Answer: A

Explanation:

Microsoft Defender for Cloud Apps is now part of Microsoft 365 Defender, which correlates signals from across the Microsoft Defender suite and provides incident-level detection, investigation, and powerful response capabilities. For more information, see Microsoft Defender for Cloud Apps in Microsoft 365 Defender.

Question: 200 CertyIQ

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

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

You have an Amazon Web Services (AWS) account, a Google Workspace subscription, and a GitHub account.

You deploy an Azure subscription and enable Microsoft 365 Defender.

You need to ensure that you can monitor OAuth authentication requests by using Microsoft Defender for Cloud Apps.

Solution: From the Microsoft 365 Defender portal, you add the Microsoft Azure app connector.

Does this meet the goal?

A.Yes

B.No

Answer: B

Explanation:

Correct Answer. B, No. The way to manage those third party apps is through the Microsoft Defender for Cloud Apps -> App Connector. If not, there is no way to detect and investigate them.

https://learn.microsoft.com/en-us/defender-cloud-apps/manage-app-permissions

Question: 201 CertyIQ

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

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

You have an Amazon Web Services (AWS) account, a Google Workspace subscription, and a GitHub account.

You deploy an Azure subscription and enable Microsoft 365 Defender.

You need to ensure that you can monitor OAuth authentication requests by using Microsoft Defender for Cloud Apps.

Solution: From the Microsoft 365 Defender portal, you add the Amazon Web Services app connector.

Does this meet the goal?

A.Yes
B.No

Answer: B

Explanation:

Reference:

https://learn.microsoft.com/en-us/defender-cloud-apps/manage-app-permissions

Question: 202 CertyIQ

Your company purchases a Microsoft 365 E5 subscription.

A user named User1 is assigned the Security Administrator role.

You need to ensure that User1 can create Microsoft Defender for Cloud Apps session policies.

What should you do first?

A.Create a Conditional Access policy and select Require app protection policy.
B.Create a Conditional Access policy and select Use Conditional Access App Control.
C.Assign the Cloud Application Administrator role to User1.
D.Assign the Cloud App Security Administrator role to User1.

Answer: B

Explanation:

Answer . B. Create a Conditional Access policy and select Use Conditional Access App Control. "The relevant apps should be deployed with Conditional Access App Control"Make sure you've configured your IdP solution to work with Defender for Cloud Apps, as follows:- For Azure AD Conditional Access, see Configure integration with Azure AD- For other IdP solutions, see Configure integration with other IdP solutions"

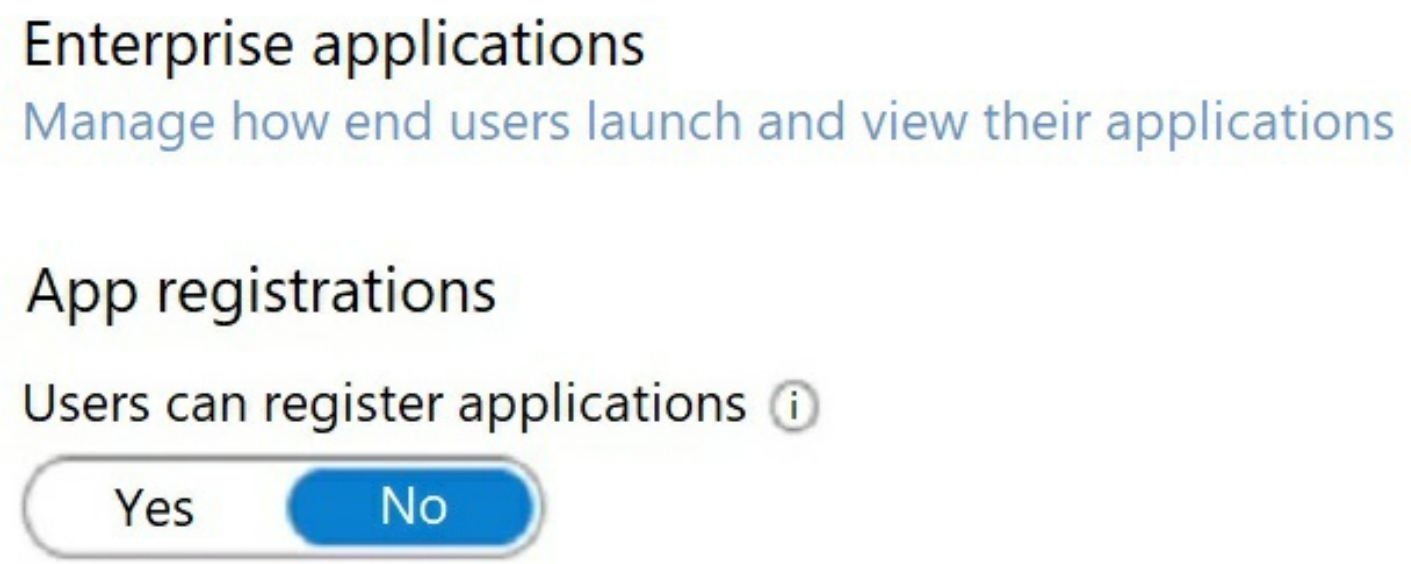
References:

https://learn.microsoft.com/en-us/defender-cloud-apps/session-policy-aad#prerequisites-to-using-session-policies

Question: 203 CertyIQ

You have an Azure subscription that contains a user named User1.

The App registration settings for the Azure AD tenant are configured as shown in the following exhibit.



User1 builds an ASP.NET web app named App1.

You need to ensure that User1 can register App1. The solution must use the principle of least privilege.

Which role should you assign to User1?

A.Application Developer
B.Cloud App Security Administrator
C.Cloud Application Administrator
D.Application Administrator

Answer: A

Explanation:

"Assign the Application Developer role to grant the ability to create application registrations when the Users can register applications setting is set to No. This role also grants permission to consent on one's own behalf when the Users can consent to apps accessing company data on their behalf setting is set to No.

"https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/delegate-app-roles#grant-individual-permissions-to-create-and-consent-to-applications-when-the-default-ability-is-disabled

Question: 204 CertyIQ

HOTSPOT
-

You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Location
RG1	Resource group	East US
Managed1	Managed identity	East US
Managed2	Managed identity	West US

The subscription contains the virtual machines shown in the following table.

Name	Location	Identity
VM1	East US	System-assigned
VM2	West US	System-assigned
VM3	East US	Managed1
VM4	West US	*None*

Which identities can be assigned the Owner role for RG1, and to which virtual machines can you assign Managed2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Identities with Owner role:

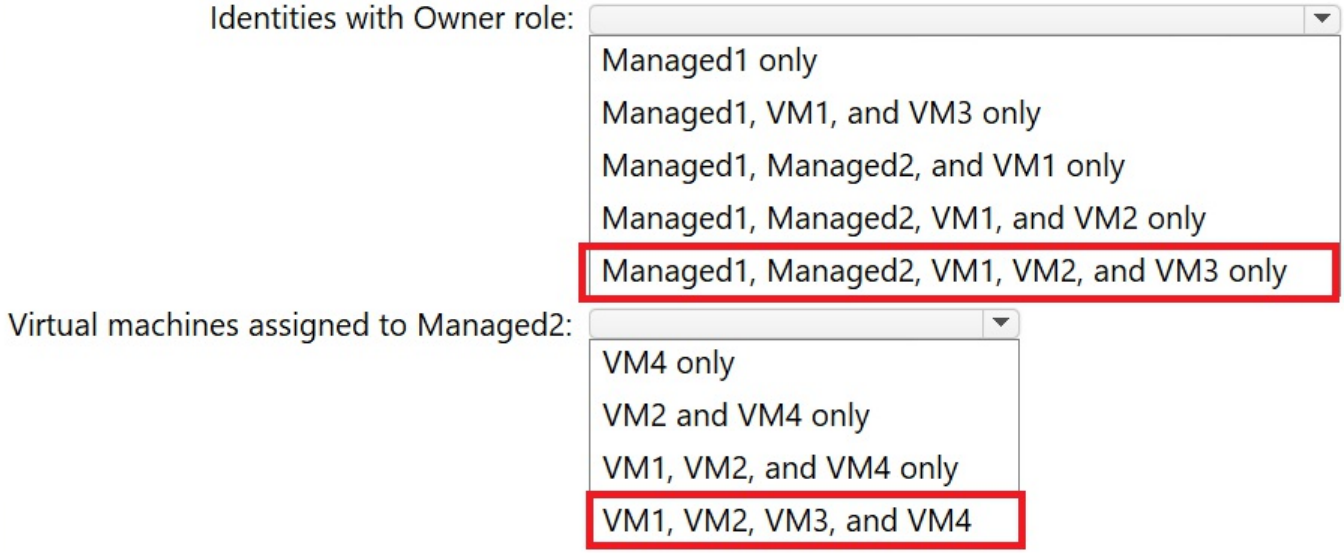
- Managed1 only
- Managed1, VM1, and VM3 only
- Managed1, Managed2, and VM1 only
- Managed1, Managed2, VM1, and VM2 only
- Managed1, Managed2, VM1, VM2, and VM3 only

Virtual machines assigned to Managed2:

- VM4 only
- VM2 and VM4 only
- VM1, VM2, and VM4 only
- VM1, VM2, VM3, and VM4

Answer:

Answer Area



Explanation:

Box 1 Managed1,Managed2,VM1,VM2 and VM3 only.

Box 2 VM1,VM2,VM3 and VM4.

Question: 205 CertyIQ

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

You plan to increase app security for the subscription.

You need to identify which apps do NOT require user authentication.

What should you do in the Microsoft 365 Defender portal?

A.Review the cloud app catalog.
B.Create an OAuth policy and review alerts.
C.Create a snapshot Cloud Discovery report.
D.Create a discovered app query.

Answer: A

Explanation:

A is the right answer>Tested and confirmed you can filter to see apps that require user authentication from both cloud app catalog and Cloud discovery.

2. To identify which apps do NOT require user authentication in the Microsoft 365 Defender portal, you should review the cloud app catalog. Reviewing the cloud app catalog in the Microsoft 365 Defender portal provides you with a comprehensive list of all the apps connected to your Microsoft 365 environment. It allows you to see which apps require user authentication and which ones do not.

Question: 206 CertyIQ

HOTSPOT

-

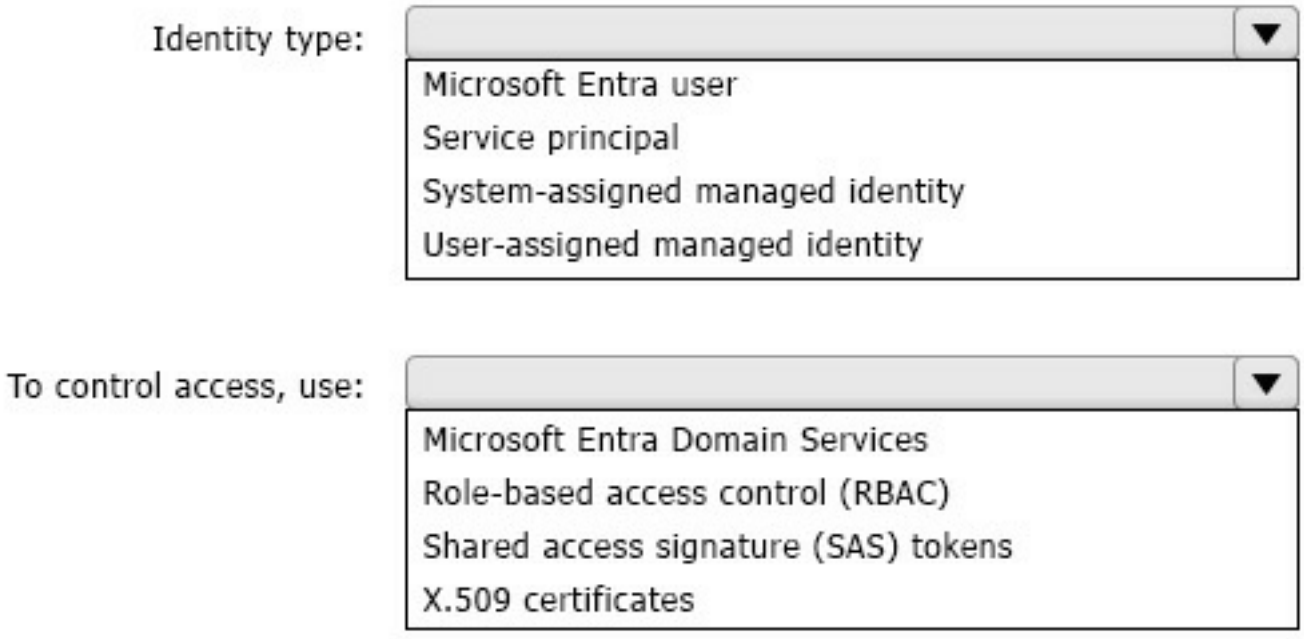
You have a Microsoft Entra tenant that contains multiple storage accounts.

You plan to deploy multiple Azure App Service apps that will require access to the storage accounts.

You need to recommend an identity solution to provide the apps with access to the storage accounts. The solution must minimize administrative effort.

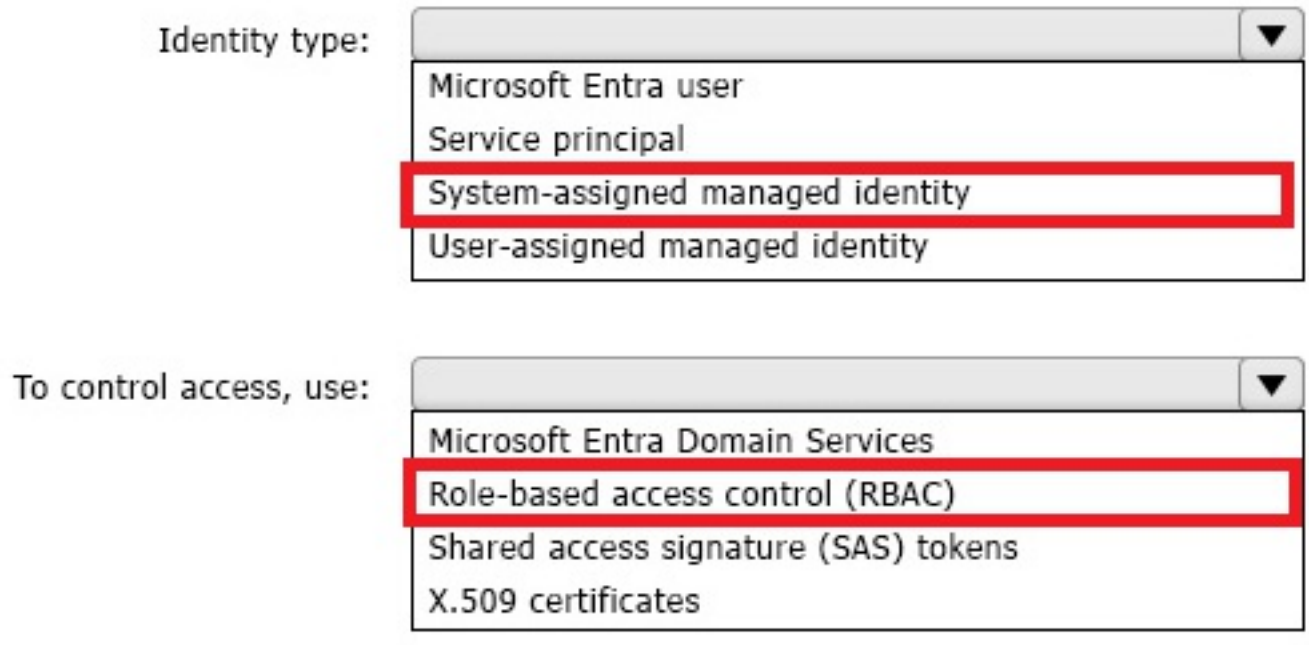
Which type of identity should you recommend, and what should you recommend using to control access to the storage accounts? To answer, select the appropriate options in the answer area.

Answer Area



Answer:

Answer Area



Explanation:

system assigned managed identity.

Role based access Control (RBAC)

https://learn.microsoft.com/en-us/azure/app-service/scenario-secure-app-access-storage?tabs=azure-portal

Question: 207 CertyIQ

You have an Azure subscription named Sub1 that contains a resource group named RG1. RG1 contains an Azure Cosmos DB database named DB1 and an Azure Kubernetes Service (AKS) cluster named AKS1. AKS1 uses a managed identity.

You need to ensure that AKS1 can access DB1. The solution must meet the following requirements:

•Ensure that AKS1 uses the managed identity to access DB1.
•Follow the principle of least privilege.

Which role should you assign to the managed identity of AKS1?

A.For Sub1, assign the Owner role.
B.For DB1, assign the Azure Cosmos DB Account Reader Role role.
C.For RG1, assign the Azure Cosmos DB Data Reader Role role.
D.For RG1, assign the Reader role.

Answer: B

Explanation:

For DB1, assign the Azure Cosmos DB Account Reader Role role.

Question: 208 CertyIQ

You have an Azure subscription that contains a storage account named storage1 and a web app named WebApp1. WebApp1 uses a system-assigned managed identity.

You need to ensure that WebApp1 can read and write files to storage1 by using the system-assigned managed identity.

What should you configure for storage1 in the Azure portal?

A.data protection
B.a shared access signature (SAS)
C.the Access control (IAM) settings
D.the File share settings
E.access keys

Answer: C

Explanation:

Access control (IAM) settings in Azure allow you to manage access to various resources within your Azure subscription. If you want to ensure that the WebApp1 web app can read and write files in storage1, you must grant the web app the appropriate permissions on the storage1 storage account.By configuring access control (IAM) for the storage account "storage1", you can assign the necessary permissions (such as "Storage Blob

Data Contributor" or "Storage Blob Data Reader") to the web app's managed identity to access the Blob services can access to read and write files.

Question: 209 CertyIQ

HOTSPOT
-

You have an Azure subscription named Sub1 that contains a storage account named storage1.

You need to deploy two apps named App1 and App2 that will have the following configurations:

•App1 will be deployed as a registered app in Sub1.
•App1 will access storage1 by using Microsoft Entra authentication.
•App2 will access storage1 by using a single Microsoft Entra identity.
•App2 be hosted on two new virtual machines named VM1 and VM2.

The solution must minimize administrative effort.

Which type of identity will each app use to access storage1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

App1:

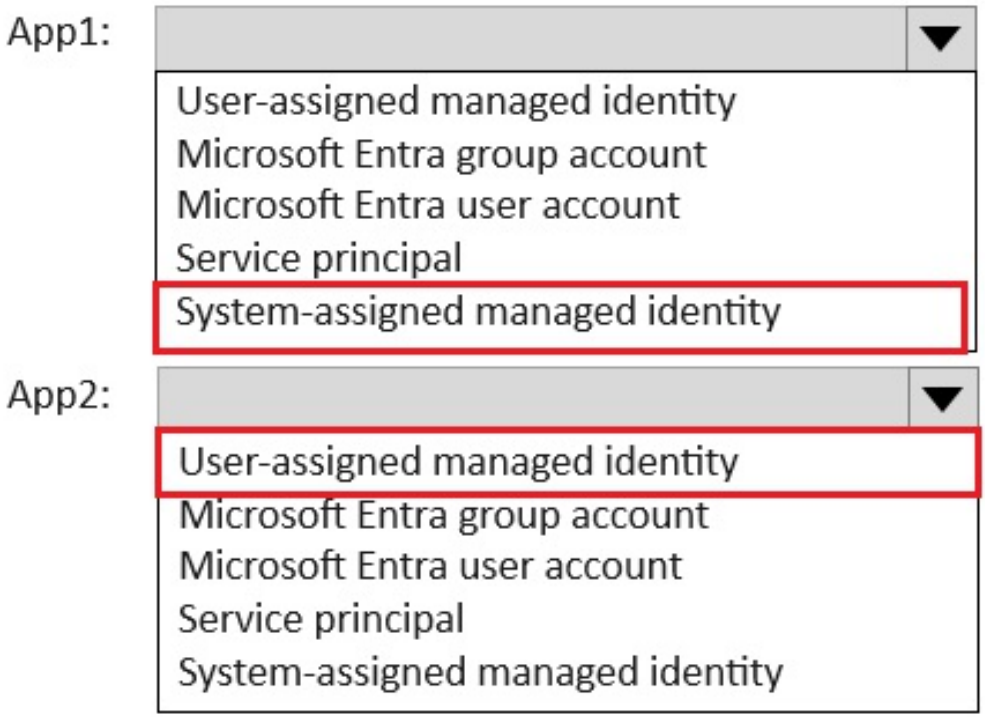
- User-assigned managed identity
- Microsoft Entra group account
- Microsoft Entra user account
- Service principal
- System-assigned managed identity

App2:

- User-assigned managed identity
- Microsoft Entra group account
- Microsoft Entra user account
- Service principal
- System-assigned managed identity

Answer:

Answer Area



Question: 210

CertyIQ

HOTSPOT
-

You have a Microsoft 365 E5 subscription.

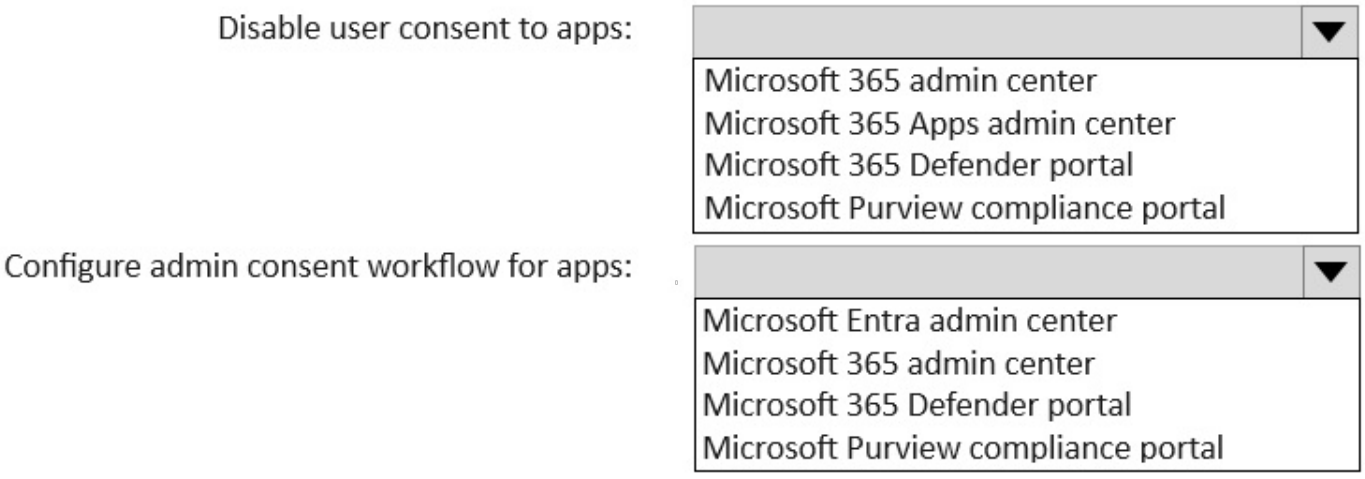
You need to configure app consent for the subscription. The solution must meet the following requirements:

•Disable user consent to apps.
•Configure admin consent workflow for apps.

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

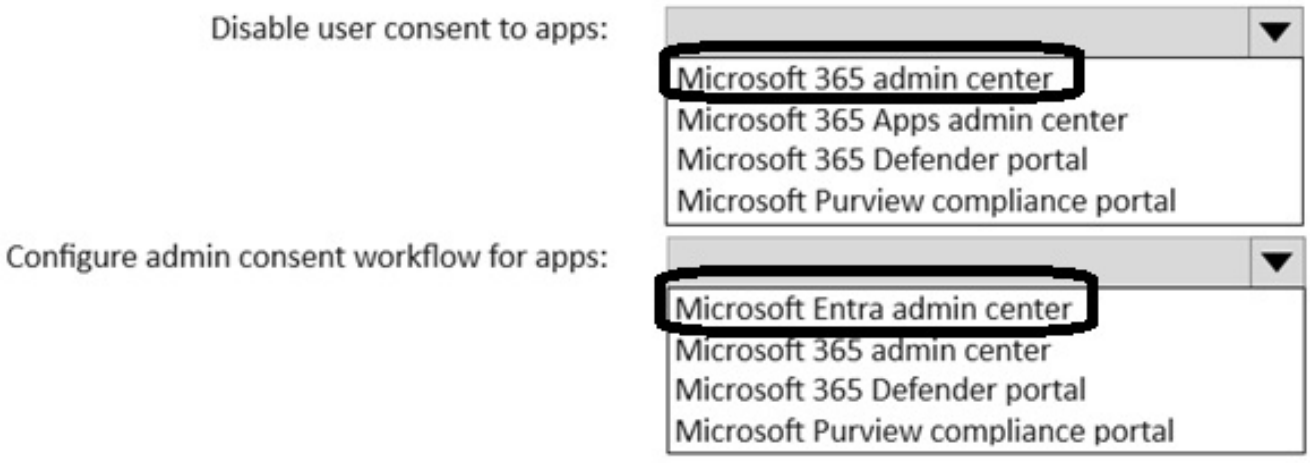
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area



Question: 211 CertyIQ

You have a Microsoft 365 subscription.

You plan to deploy an app named App1 that will have the following configurations:

•Will be registered in Microsoft Entra
•Will access the signed-in user's Microsoft Outlook calendar by using the Microsoft Graph API

You need to ensure that App1 can access Microsoft Graph.

What should you use?

A.application permissions
B.delegated permissions
C.a custom role-based access control (RBAC) role
D.a built-in role-based access control (RBAC) role

Answer: B

Explanation:

Correct answer is B:delegated permissions.

Question: 212 CertyIQ

You have a Microsoft 365 tenant.
In Azure Active Directory (Azure AD), you configure the terms of use.
You need to ensure that only users who accept the terms of use can access the resources in the tenant. Other users must be denied access.
What should you configure?

A. an access policy in Microsoft Cloud App Security.
B. Terms and conditions in Microsoft Endpoint Manager.
C. a conditional access policy in Azure AD
D. a compliance policy in Microsoft Endpoint Manager

Answer: C

Explanation:

Conditional access is correct.

See the link "How to deploy terms of use policy in AZAD" referenced in the MS article;

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use

Question: 213 CertyIQ

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

Name	Type	Membership type
Group1	Security	Assigned
Group2	Security	Dynamic User
Group3	Security	Dynamic Device
Group4	Microsoft 365	Assigned
Group5	Microsoft 365	Dynamic User

For which groups can you create an access review?

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

Answer: D

Explanation:

You cannot create access reviews for device groups.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review

Question: 214 CertyIQ

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

Name	Type	Member of
User1	Member	Group1
User2	Member	Group1
User3	Guest	Group1

User1 is the owner of Group1.
You create an access review that has the following settings:
- Users to review: Members of a group
- Scope: Everyone
- Group: Group1
- Reviewers: Members (self)

Which users can perform access reviews for User3?

A. User1, User2, and User3

B. User3 only

C. User1 only

D. User1 and User2 only

Answer: B

Explanation:

- When Reviewers is set to Members (Self), then only each individual member can review their own access, and if they do not then it is reported as no response

- [https://learn.microsoft.com/en-us/azure/active-directory/governance/create-access-review] (https://learn.microsoft.com/en-us/azure/active-directory/governance/create-access-review)

- [https://learn.microsoft.com/en-us/azure/active-directory/governance/create-access-review] (https://learn.microsoft.com/en-us/azure/active-directory/governance/create-access-review)

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-start-security-review

Question: 215 CertyIQ

HOTSPOT -
You have an Azure Active Directory (Azure AD) tenant that contains Azure AD Privileged Identity Management (PIM) role settings for the User administrator role as shown in the following exhibit.

... ContosoAzureAD > Identity Governance > Privileged Identity Management > ContosoAzureAD > User Administrator >

Role setting details - User Administrator

Privileged Identity Management | Azure AD roles

Edit

Activation

SETTING	STATE
Activation maximum duration (hours)	8 hour(s)
Require justification on activation	Yes
Require ticket information on activation	No
On activation, require Azure MFA	Yes
Require approval to activate	Yes
Approvers	None

Assignment

SETTING	STATE
Allow permanent eligible assignment	No
Expire eligible assignments after	15 day(s)
Allow permanent active assignment	No
Expire active assignments after	1 month(s)
Require Azure Multi-Factor Authentication on active assignment	No
Require justification on active assignment	No

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

A user who requires access to the User administration role must perform multi-factor authentication (MFA) every **[answer choice]**.

- 8 hours
- 15 days
- 1 month

Before an eligible user can perform a task that requires the User administrator role, the activation must be approved by a **[answer choice]**.

- global administrator only
- global administrator or privileged role administrator
- permanently assigned user administrator
- privileged role administrator only

Answer:

Answer Area

A user who requires access to the User administration role must perform multi-factor authentication (MFA) every **[answer choice]**.

- 8 hours
- 15 days
- 1 month

Before an eligible user can perform a task that requires the User administrator role, the activation must be approved by a **[answer choice]**.

- global administrator only
- global administrator or privileged role administrator
- permanently assigned user administrator
- privileged role administrator only

Explanation:

8 hours

Global administrators and privileged role administrators

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-deployment-plan

Question: 216

CertyIQ

HOTSPOT -
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains a user named User1.
User1 has the devices shown in the following table.

Name	Platform	Registered in contoso.com
Device1	Windows 10	Yes
Device2	Windows 10	No
Device3	iOS	Yes

On November 5, 2020, you create and enforce terms of use in contoso.com that has the following settings:
- Name: Terms1
- Display name: Contoso terms of use
- Require users to expand the terms of use: On

- Require users to consent on every device: On
- Expire consents: On
- Expire starting on: December 10, 2020
- Frequency: Monthly

On November 15, 2020, User1 accepts Terms1 on Device3.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

Statements	Yes	No
On November 20, 2020, User1 can accept Terms1 on Device1.	○	○
On December 11, 2020, User1 can accept Terms1 on Device2.	○	○
On December 7, 2020, User1 can accept Terms1 on Device3.	○	○

Answer:

Answer Area

Statements	Yes	No
On November 20, 2020, User1 can accept Terms1 on Device1.	○	○
On December 11, 2020, User1 can accept Terms1 on Device2.	○	○
On December 7, 2020, User1 can accept Terms1 on Device3.	○	○

Explanation:

Box 1: Yes because User1 has not yet accepted the terms on Device1.

Box 2: No, Answer date is December 11, 2020 expire starting on: December 10, 2020 answer date is December 11, 2020

Box 3: No because User1 has already accepted the terms on Device3. The terms do not expire until December 10 and then monthly after that.

Question: 217 CertyIQ

Your company recently implemented Azure Active Directory (Azure AD) Privileged Identity Management (PIM).
While you review the roles in PIM, you discover that all 15 users in the IT department at the company have permanent security administrator rights.
You need to ensure that the IT department users only have access to the Security administrator role when required.
What should you configure for the Security administrator role assignment?

A. Expire eligible assignments after from the Role settings details
B. Expire active assignments after from the Role settings details
C. Assignment type to Active
D. Assignment type to Eligible

Answer: D

Explanation:

I think the best way to read this question is "What should you configure FIRST for the Security administrator role assignment?"

You would setup "D. Assignment type to Eligible" so the admins can request the role in future, for a limited time based on the Role Setting of "Activation maximum duration (hours): 8 (by default)"

Only then would you set "B. Expire active assignments after from the Role settings details"

So D is the correct answer.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

Question: 218 CertyIQ

You have a Microsoft 365 tenant.
The Sign-ins activity report shows that an external contractor signed in to the Exchange admin center.
You need to review access to the Exchange admin center at the end of each month and block sign-ins if required.
What should you create?

A. an access package that targets users outside your directory
B. an access package that targets users in your directory
C. a group-based access review that targets guest users
D. an application-based access review that targets guest users

Answer: C

Explanation:

You can target a group with a conditional policy to detect and remediate the login at the end of each month

Not valid, A, B, D

D admin is not using an app is using a privileged role to use Exchange admin center

A and B No

An access package.

A bundle of resources that a team or project needs and is governed with policies. Access packages are defined in containers called catalogs.

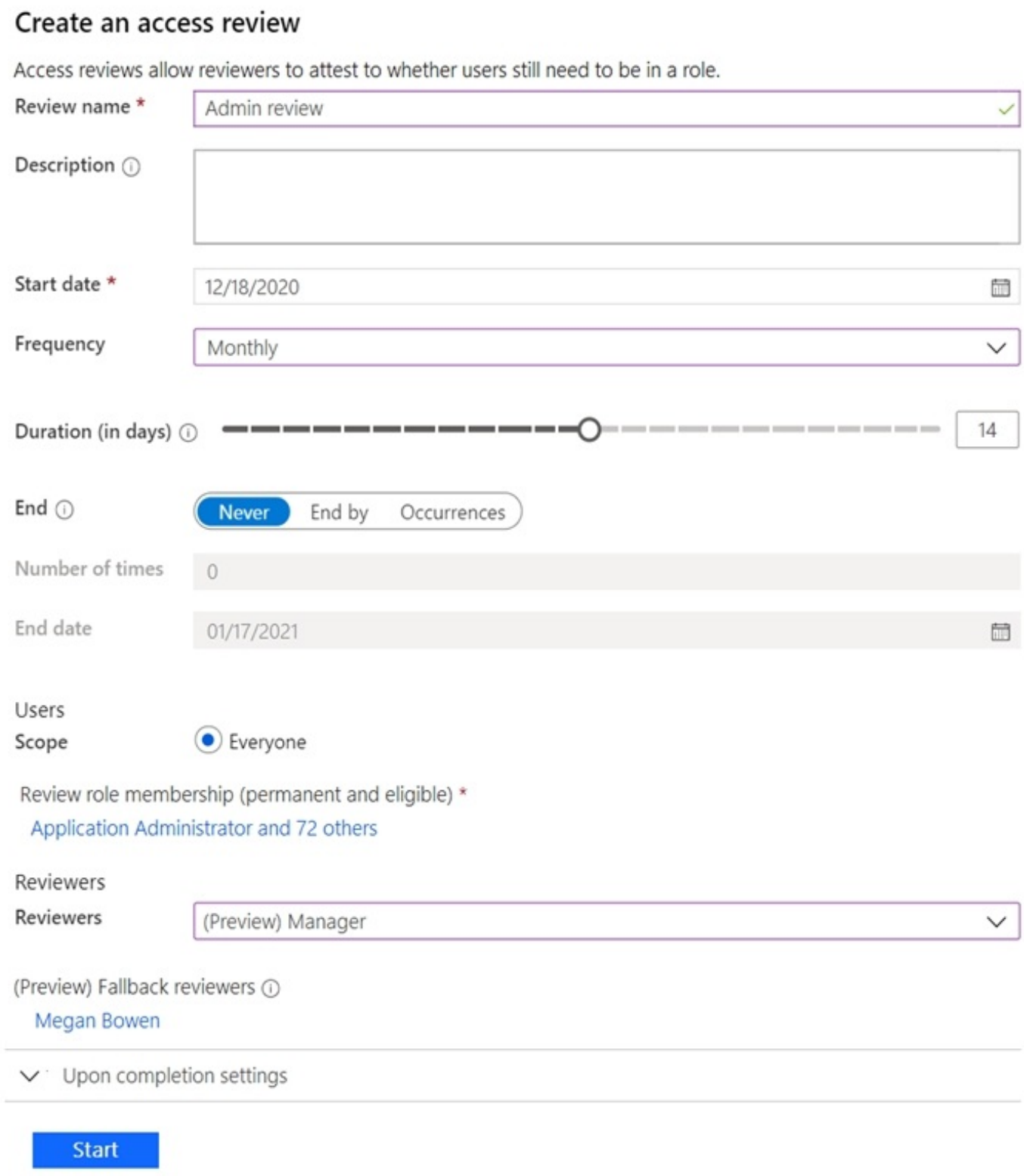
To reduce the risk of stale access, you should enable periodic reviews of users who have active assignments to an access package in Azure AD entitlement management

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview

Question: 219 CertyIQ

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 tenant.
You have 100 IT administrators who are organized into 10 departments.
You create the access review shown in the exhibit. (Click the Exhibit tab.)



You discover that all access review requests are received by Megan Bowen.

You need to ensure that the manager of each department receives the access reviews of their respective department.
Solution: You create a separate access review for each role.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

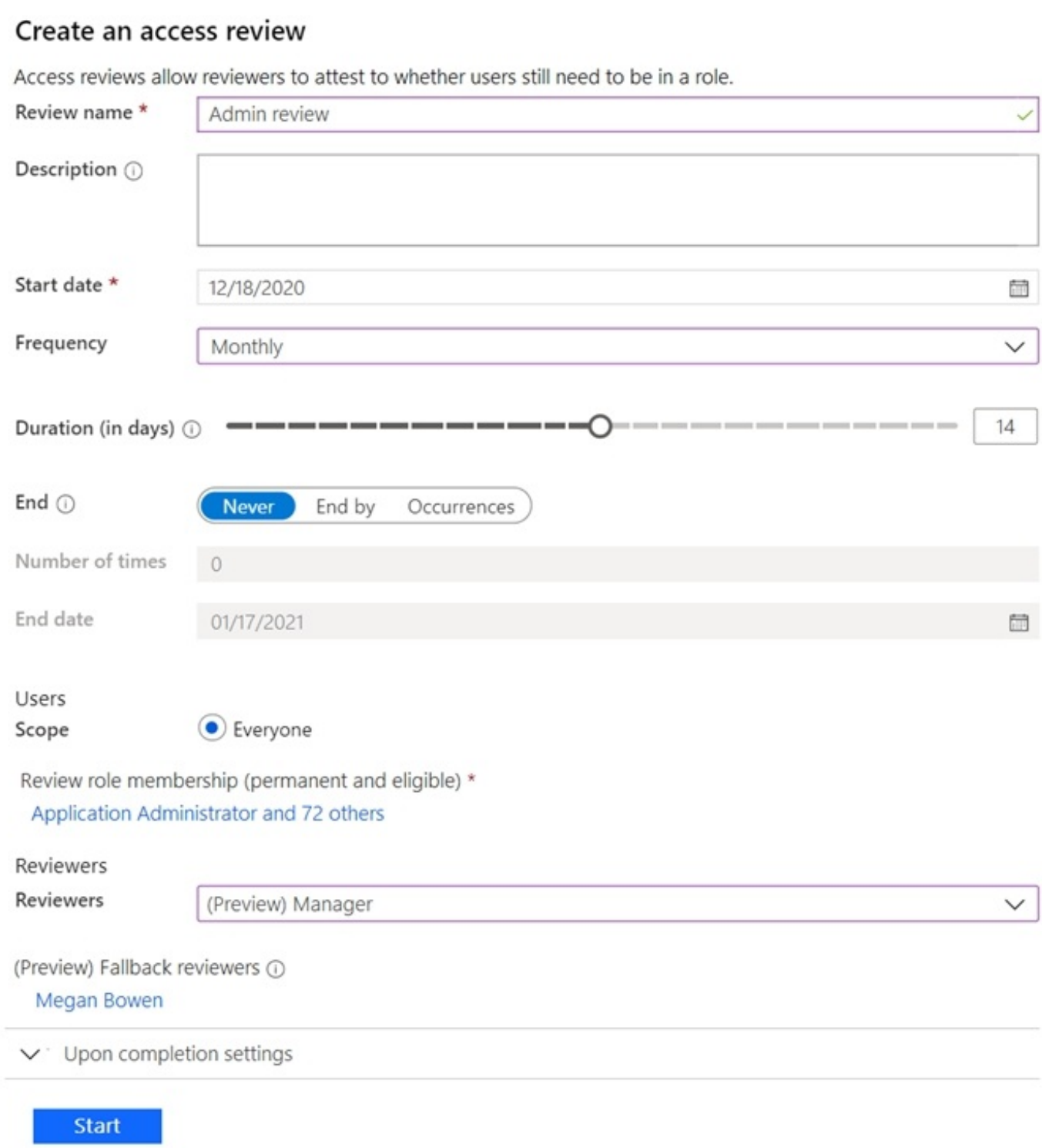
No - each access review would still send review approval to Megan as no manager has been set for the user accounts under review.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review

Question: 220 CertyIQ

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 tenant.
You have 100 IT administrators who are organized into 10 departments.
You create the access review shown in the exhibit. (Click the Exhibit tab.)



You discover that all access review requests are received by Megan Bowen.
You need to ensure that the manager of each department receives the access reviews of their respective department.
Solution: You modify the properties of the IT administrator user accounts.
Does this meet the goal?

A. Yes

B. No

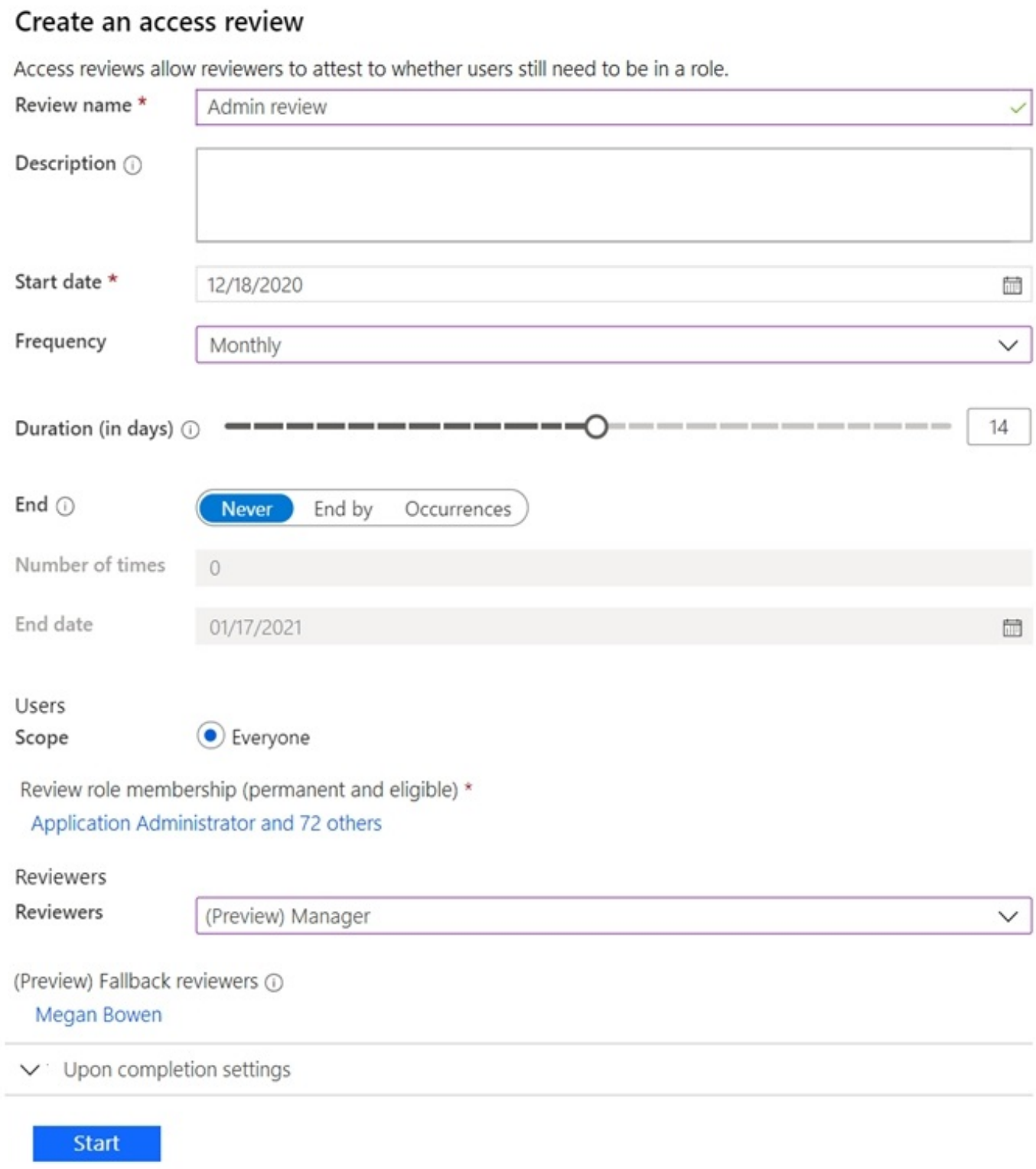
Answer: A

Explanation:

Yes. Megan Bowen is receiving the access reviews because no Managers are set for those users under Job Info, she is the fallback reviewer. If you set the Manager value to a user, this user will receive the review instead of Megan Bowen.

Question: 221 CertyIQ

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 tenant.
You have 100 IT administrators who are organized into 10 departments.
You create the access review shown in the exhibit. (Click the Exhibit tab.)



You discover that all access review requests are received by Megan Bowen.
You need to ensure that the manager of each department receives the access reviews of their respective department.
Solution: You set Reviewers to Member (self).
Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Fallback reviewers are asked to do a review when the user has no manager specified in the directory or the group does not have an owner

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review

Question: 222 CertyIQ

You have a Microsoft 365 tenant.
The Azure Active Directory (Azure AD) tenant syncs to an on-premises Active Directory domain.
You plan to create an emergency-access administrative account named Emergency1. Emergency1 will be assigned the Global administrator role in Azure AD.
Emergency1 will be used in the event of Azure AD functionality failures and on-premises infrastructure failures.
You need to reduce the likelihood that Emergency1 will be prevented from signing in during an emergency.
What should you do?

A. Configure Azure Monitor to generate an alert if Emergency1 is modified or signs in.

B. Require Azure AD Privileged Identity Management (PIM) activation of the Global administrator role for Emergency1.

C. Configure a conditional access policy to restrict sign-in locations for Emergency1 to only the corporate network.

D. Configure a conditional access policy to require multi-factor authentication (MFA) for Emergency1.

Answer: A

Explanation:

This is an account used in 'break the glass' scenarios. It only has a very long password, that is kept under lock and key. User id and password are not connected to any user or device for authentication. No MFA can block its access. Even with Cell or network/email/phone down situations you can login with this account. You can login from anywhere. So it needs to be monitored to prevent tampering and account usage.

Question: 223 CertyIQ

You have an Azure Active Directory (Azure AD) tenant named contoso.com.
You implement entitlement management to provide resource access to users at a company named Fabrikam, Inc.
Fabrikam uses a domain named fabrikam.com.
Fabrikam users must be removed automatically from the tenant when access is no longer required.
You need to configure the following settings:
- Block external user from signing in to this directory: No
- Remove external user: Yes
- Number of days before removing external user from this directory: 90

What should you configure on the Identity Governance blade?

A. Access packages

B. Entitlement management settings

C. Terms of use

D. Access reviews settings

Answer: B

Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-external-users

Question: 224 CertyIQ

You have an Azure Active Directory (Azure AD) P1 tenant.
You need to review the Azure AD sign-in logs to investigate sign-ins that occurred in the past.
For how long does Azure AD store events in the sign-in logs?

A. 14 days

B. 30 days

C. 90 days

D. 365 days

Answer: B

Explanation:

To be selected in the exam, to add, free, No, because no 7 days, but to choose 30 or 90 they need to add P1 or P2, but assume P2 is more expensive so thought only just P1, so 30 is correct

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/reference-reports-data-retention#how-long-does-azure-ad-store-the-data

Question: 225 CertyIQ

You have an Azure subscription that contains the resources shown in the following table.

Name	Type
Group1	Group that has the Assigned membership type
App1	Enterprise application in Azure Active Directory (Azure AD)
Contributor	Azure subscription role
Role1	Azure Active Directory (Azure AD) role

For which resources can you create an access review?

A. Group1, Role1, and Contributor only

B. Group1 only

C. Group1, App1, Contributor, and Role1

D. Role1 and Contributor only

Answer: C

Explanation:

Yeah, it is possible to create access reviews for both Azure AND Azure AD roles.

Tested in Azure portal.

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-create-azure-ad-roles-and-resource-roles-review

Access reviews require an Azure AD Premium P2 license.

Access reviews for Group1 and App1 can be configured in Azure AD Access Reviews.

Access reviews for the Contributor role and Role1 would need to be configured in Privileged Identity Management (PIM). PIM is included in Azure AD Premium

P2.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-start-security-review?toc=/azure/active-directory/governance/ toc.json https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview

Question: 226 CertyIQ

You have an Azure Active Directory (Azure AD) tenant that uses conditional access policies.
You plan to use third-party security information and event management (SIEM) to analyze conditional access usage.
You need to download the Azure AD log by using the administrative portal. The log file must contain changes to conditional access policies.
What should you export from Azure AD?

A. audit logs in CSV format
B. sign-ins in CSV format
C. audit logs in JSON format
D. sign-ins in JSON format

Answer: C

Explanation:

You can also choose to download the filtered data, up to 250,000 records, by selecting the Download button. You can download the logs in either CSV or JSON format

So this question, can be one of those that you will got Corect if you choose any of both csv or JSON,

You can use the JSON transform feature in the Power Query Editor in Excel to split each property in the JSON object in the AuditData column into multiple columns so that each property has its own column.

So answer= C, JSON

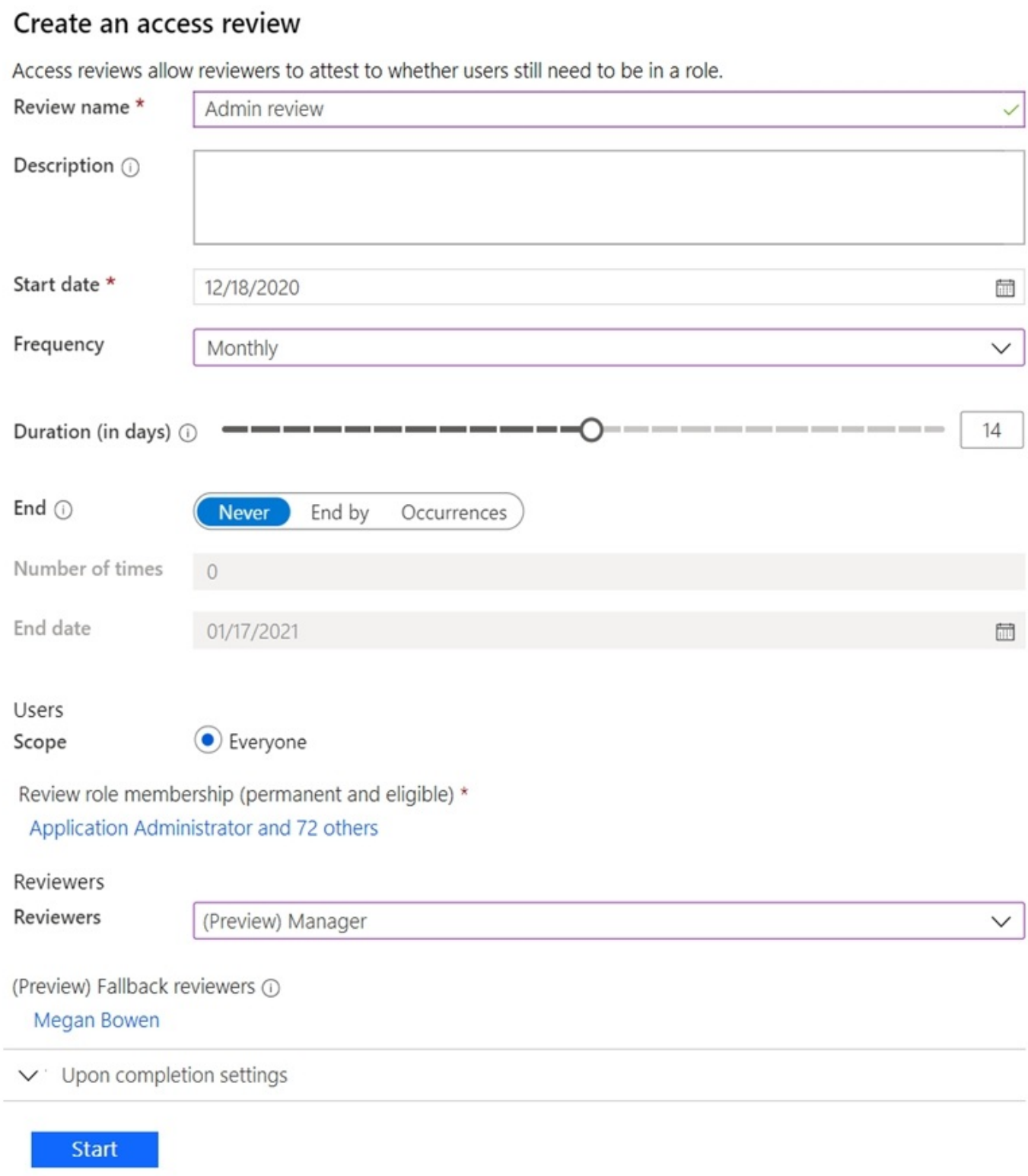
https://docs.microsoft.com/en-us/microsoft-365/compliance/export-view-audit-log-records?view=o365-worldwide

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-audit-logs

Question: 227 CertyIQ

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 tenant.
You have 100 IT administrators who are organized into 10 departments.
You create the access review shown in the exhibit. (Click the Exhibit tab.)



You discover that all access review requests are received by Megan Bowen.

You need to ensure that the manager of each department receives the access reviews of their respective department.
Solution: You add each manager as a fallback reviewer.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

The option of Fallback reviewer is when you set as reviewer to the manager or group owner and somehow that user is not having a manager in the directory. In those case, the fallback reviewer, which could be a department head would be the reviewer.

"Fallback reviewers are asked to do a review when the user has no manager specified in the directory or the group does not have an owner."

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review

Question: 228 CertyIQ

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

Name	Type
User1	User
Guest1	Guest
Identity1	Managed identity

Which objects can you add as eligible in Azure AD Privileged Identity Management (PIM) for an Azure AD role?

A. User1, Guest1, and Identity1
B. User1 and Guest1 only
C. User1 only
D. User1 and Identity1 only

Answer: B

Explanation:

You cannot assign service principals as eligible to Azure AD roles, Azure roles, and Privileged Access groups but you can grant a time limited active assignment to all three.

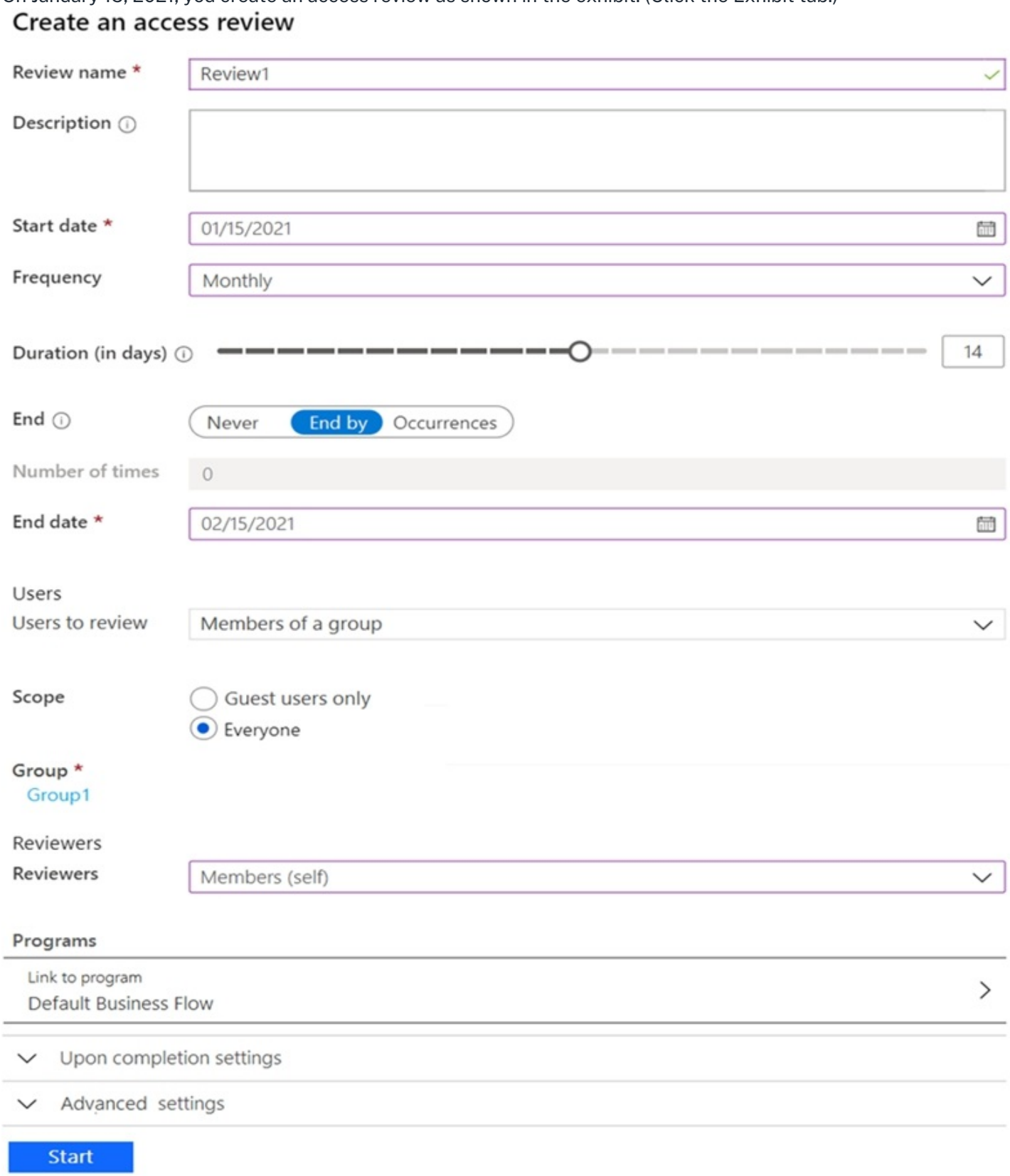
Reference:

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-deployment-plan

Question: 229 CertyIQ

HOTSPOT -
You have an Azure Active Directory (Azure AD) tenant that contains the following group:
- Name: Group1
- Members: User1, User2
- Owner: User3

On January 15, 2021, you create an access review as shown in the exhibit. (Click the Exhibit tab.)



Users answer the Review1 question as shown in the following table.

User	Date	Do you still need access to Group1?
User1	January 17, 2021	Yes
User2	January 20, 2021	No

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

NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

Statements	Yes	No
On February 5, 2021, User1 can answer the Review1 question again.	○	○
On January 25, 2021, User2 can answer the Review1 question again.	○	○
On January 22, 2021, User3 can answer the Review1 question.	○	○

Answer:

Answer Area

Statements	Yes	No
On February 5, 2021, User1 can answer the Review1 question again.	○	○
On January 25, 2021, User2 can answer the Review1 question again.	○	○
On January 22, 2021, User3 can answer the Review1 question.	○	○

Explanation:

#1 No, because as it's rolling "monthly" review cycle with an end date, the review period which is eligible for input or change is a 14 day period, since User 1 responded in the first period which started 15th Jan and ended 29th Jan, to respond 5th Feb would be outside of this scope.

#2 Yes, Similar to #1 for User1, this is within the 14 day period of User2.

#3 No, Reviews are for Group1, which User3 is not a member of.

Reference:

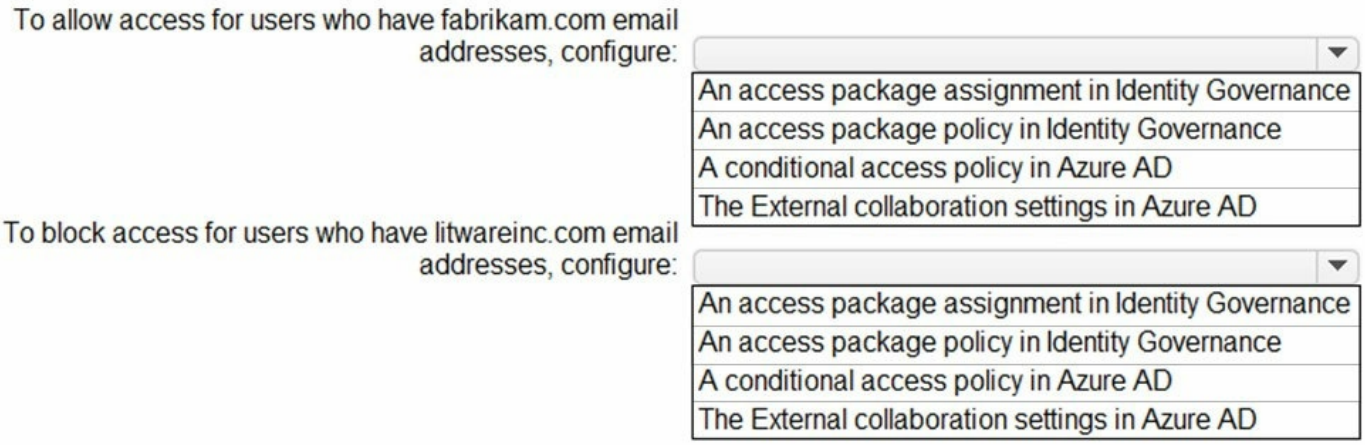
https://docs.microsoft.com/en-us/azure/active-directory/governance/review-your-access

Question: 230 CertyIQ

HOTSPOT -
Your company has an Azure Active Directory (Azure AD) tenant named contoso.com. The company has a business partner named Fabrikam, Inc.
Fabrikam uses Azure AD and has two verified domain names of fabrikam.com and litwareinc.com. Both domain names are used for Fabrikam email addresses.
You plan to create an access package named package1 that will be accessible only to the users at Fabrikam.
You create a connected organization for Fabrikam.
You need to ensure that the package1 will be accessible only to users who have fabrikam.com email addresses.

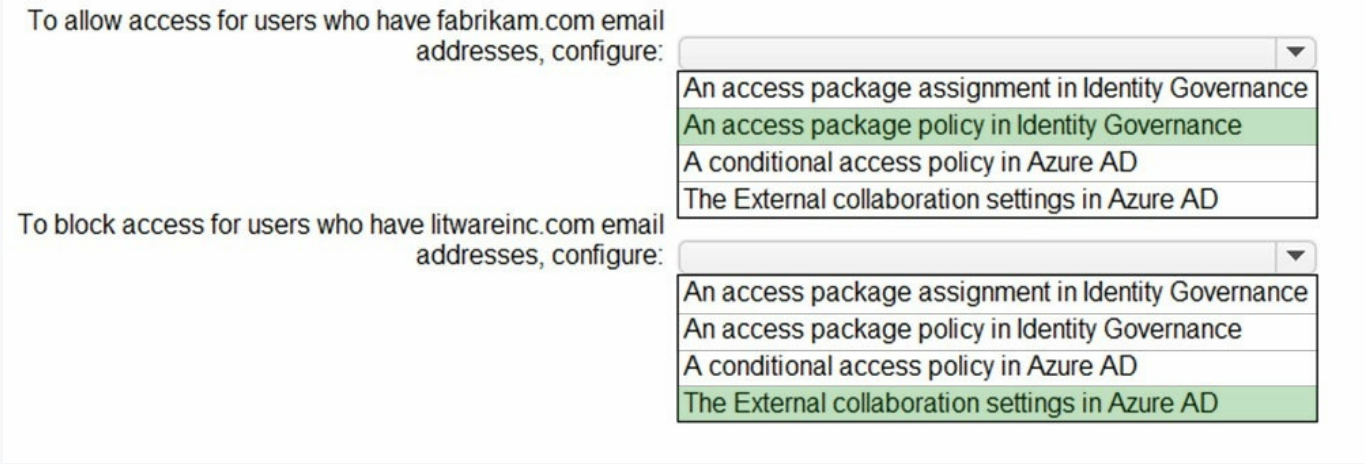
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area



Answer:

Answer Area



Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-request-policy https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-create

Question: 231 CertyIQ

You have an Azure Active Directory (Azure AD) tenant named contoso.com that has Azure AD Identity Protection policies enforced.
You create an Azure Sentinel instance and configure the Azure Active Directory connector.
You need to ensure that Azure Sentinel can generate incidents based on the risk alerts raised by Azure AD Identity Protection.
What should you do first?

A. Add a Microsoft Sentinel data connector.

B. Configure the Notify settings in Azure AD Identity Protection.

C. Create a Microsoft Sentinel playbook.

D. Modify the Diagnostics settings in Azure AD.

Answer: C

Explanation:

Add a Microsoft Sentinel Data connector is the wrong answer. Meant to mislead.

Because question itself mentions that AAD connector was added. Which seem to cover all AAD functionality including Identity Protection feature.

What you are asked to do is generate incidents based on the risk alerts.

For that you use playbooks in Sentinel. Which automates tasks that SOC engineers need to such as generte risk alerts. So answer is C.

Question: 232 CertyIQ

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You use Azure Monitor to analyze Azure Active Directory (Azure AD) activity logs.
You receive more than 100 email alerts each day for failed Azure AD user sign-in attempts.
You need to ensure that a new security administrator receives the alerts instead of you.
Solution: From Azure AD, you create an assignment for the Insights administrator role.
Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Permissions should be given to a Security Administrator or

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

Insights Administrator is an administrator Ofc365 Viva app. (Employee Experience Platform).

Question: 233 CertyIQ

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You use Azure Monitor to analyze Azure Active Directory (Azure AD) activity logs.
You receive more than 100 email alerts each day for failed Azure AD user sign-in attempts.
You need to ensure that a new security administrator receives the alerts instead of you.
Solution: From Azure AD, you modify the Diagnostics settings.
Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Diagnostic settings are in Azure Monitor. Not in AAD.

Nothing here that say's about using Defender for Cloud. Defender for cloud is a separate service. And monitoring logs would be premium paid feature. Nothing here mentions Defender for Cloud.

Question: 234 CertyIQ

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You use Azure Monitor to analyze Azure Active Directory (Azure AD) activity logs.
You receive more than 100 email alerts each day for failed Azure AD user sign-in attempts.
You need to ensure that a new security administrator receives the alerts instead of you.
Solution: From Azure Monitor, you create a data collection rule.
Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Data Collection Rules is not the way to go here.

Data Collection Rules (DCRs) define the data collection process in Azure Monitor. DCRs specify what data should be collected, how to transform that data, and where to send that data. Some DCRs will be created and managed by Azure Monitor to collect a specific set of data to enable insights and visualizations.

From <https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/data-collection-rule-overview>

Question: 235 CertyIQ

You have an Azure Active Directory Premium P2 tenant.
You create a Log Analytics workspace.
You need to ensure that you can view Azure Active Directory (Azure AD) audit log information by using Azure Monitor.
What should you do first?

A. Run the Set-AzureADTenantDetail cmdlet.

B. Create an Azure AD workbook.

C. Modify the Diagnostics settings for Azure AD.

D. Run the Get-AzureADAuditDirectoryLogs cmdlet.

Answer: C

Explanation:

Send logs to Azure Monitor

Sign in to the Azure portal.

Select Azure Active Directory > Diagnostic settings -> Add diagnostic setting. You can also select Export Settings from the Audit Logs or Sign-ins page to get to the diagnostic settings configuration page.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-integrate-activity-logs-with-log-analytics

Question: 236 CertyIQ

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

Name	Role
User1	None
User2	Privileged authentication administrator
User3	Global administrator

In Azure AD Privileged Identity Management (PIM), you configure the Global administrator role as shown in the following exhibit.

Edit

Setting	State
Activation maximum duration (hours)	1 hour(s)
vRequire justification on activation	Yes
Require ticket information on activation	No
On activation, require Azure MFA	Yes
Require approval to activate	No
Approvers	None

Assignment

Setting	State
Allow permanent eligible assignment	Yes
Expire eligible assignments after	-
Allow permanent active assignment	Yes
Expire active assignments after	-
Require Azure Multi-Factor Authentication on active assignment	No
Require justification on active assignment	Yes

User1 is eligible for the Global administrator role.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

Statements	Yes	No
User1 requires Azure Multi-Factor Authentication (MFA) to activate the Global administrator role.	○	○
User2 must approve all activation requests for the Global administrator role.	○	○
User2 and User3 can edit the Global administrator role assignment.	○	○

Answer:

Answer Area

Statements	Yes	No
User1 requires Azure Multi-Factor Authentication (MFA) to activate the Global administrator role.	○	○
User2 must approve all activation requests for the Global administrator role.	○	○
User2 and User3 can edit the Global administrator role assignment.	○	○

Explanation:
Box 1: Yes -

MFA is required on activation -

Box 2: No -
The Privileged Authentication Administrator can set or reset any authentication method for any user, including Global Administrators.
The Privileged Role Administrator can manage role assignments, including the Global Administrator role, in Azure Active Directory, as well as within Azure AD
Privileged Identity Management. In addition, this role allows management of all aspects of Privileged Identity Management and administrative units.

Box 3: No -
The Privileged Authentication Administrator can set or reset any authentication method for any user, including Global Administrators.
The Privileged Role Administrator can manage role assignments, including the Global Administrator role, in Azure Active Directory, as well as within Azure AD

Privileged Identity Management. In addition, this role allows management of all aspects of Privileged Identity Management and administrative units.

Question: 237 CertyIQ

You have a Microsoft 365 subscription that contains the following:
- An Azure Active Directory (Azure AD) tenant that has an Azure Active Directory Premium P2 license
- A Microsoft SharePoint Online site named Site1
- A Microsoft Teams team named Team1

You need to create an entitlement management workflow to manage Site1 and Team1.
What should you do first?

A. Configure an app registration.
B. Create an Administrative unit.
C. Create an access package.
D. Create a catalog.

Answer: D

Explanation:

The correct answer is D - Create a catalog

Access packages for governed applications should be in a designated catalog. If you don't already have a catalog for your application governance scenario, create a catalog in Microsoft Entra entitlement management.

https://learn.microsoft.com/en-us/azure/active-directory/governance/identity-governance-applications-deploy#deploy-entitlement-management-policies-for-automating-access-assignment

Question: 238 CertyIQ

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You use Azure Monitor to analyze Azure Active Directory (Azure AD) activity logs.
You receive more than 100 email alerts each day for failed Azure AD user sign-in attempts.
You need to ensure that a new security administrator receives the alerts instead of you.
Solution: From Azure Monitor, you modify the action group.
Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:

The correct answer is A - Yes, you modify the action group from Azure Monitor.

https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/action-groups#configure-notifications

Question: 239 CertyIQ

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

Name	Source	Member of
Group1	Cloud	Group3
Group2	Active Directory domain	None
Group3	Cloud	None

The tenant contains the users shown in the following table.

Name	Directory-synced	Member of
User1	No	Group1
User2	No	Group2
User3	Yes	Group3

You create an access review as shown in the following table.

Setting	Value
Review type	Teams + Groups
Review scope	All users
Group	Group2, Group3
Reviewers	Users review own access
If reviewers don't respond	Remove access

For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

Statements	Yes	No
User1 will be removed automatically from Group 1 if the user does not respond to the review request.	◯	◯
User 2 will be removed automatically from Group 3 if the user does not respond to the review request.	◯	◯
User 3 will be removed automatically from Group 2 if the user does not respond to the review	◯	◯

Answer:

Answer Area

Statements	Yes	No
User1 will be removed automatically from Group 1 if the user does not respond to the review request.	○	○
User 2 will be removed automatically from Group 3 if the user does not respond to the review request.	○	○
User 3 will be removed automatically from Group 2 if the user does not respond to the review	○	○

Explanation:

Box 1: No -

User1 is member of Group1. Group1 is in the cloud. Group1 is member of Group3. Group3 is in the cloud.

The access review applies to Group3, but not to Group1. The access review is setup to remove access if reviewers don't respond.

Box 2: No -

User 1 is in group 1 outside the scope of the review

User 2 is not in group 3 so can't be removed from a group not a member of

User 3 not in group 2 so can't be removed from a group not a member of

Box 3: No -

User3 is member of Group3, not of Group2.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview

Question: 240 CertyIQ

You have a Microsoft 365 E5 subscription that contains a web app named App1.
Guest users are regularly granted access to App1.
You need to ensure that the guest users that have NOT accessed App1 during the past 30 days have their access removed. The solution must minimize administrative effort.
What should you configure?

A. a Conditional Access policy
B. a compliance policy
C. a guest access review
D. an access review for application access

Answer: D

Explanation:
Access to groups and applications for employees and guests changes over time. To reduce the risk associated with stale access assignments, administrators can use Azure Active Directory (Azure AD) to create access reviews for group members or application access.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review

Question: 241 CertyIQ

HOTSPOT -
You have an Azure Active Directory (Azure AD) ten-ant: that contains the groups shown in the following table.

Name	Owner	Number of internal users	Number of guest users
Group1	User1	500	25
Group2	User2	295	100

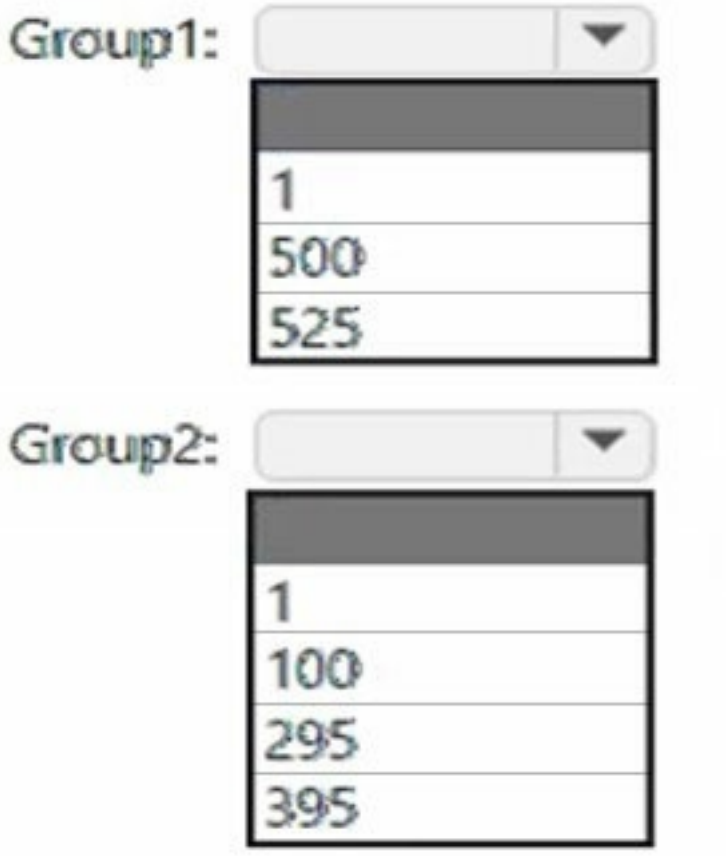
You create an access review for Group1 as shown in the following table.

Setting	Value
Review type	Teams + Groups
Review scope	All users
Reviewers	Users review own access

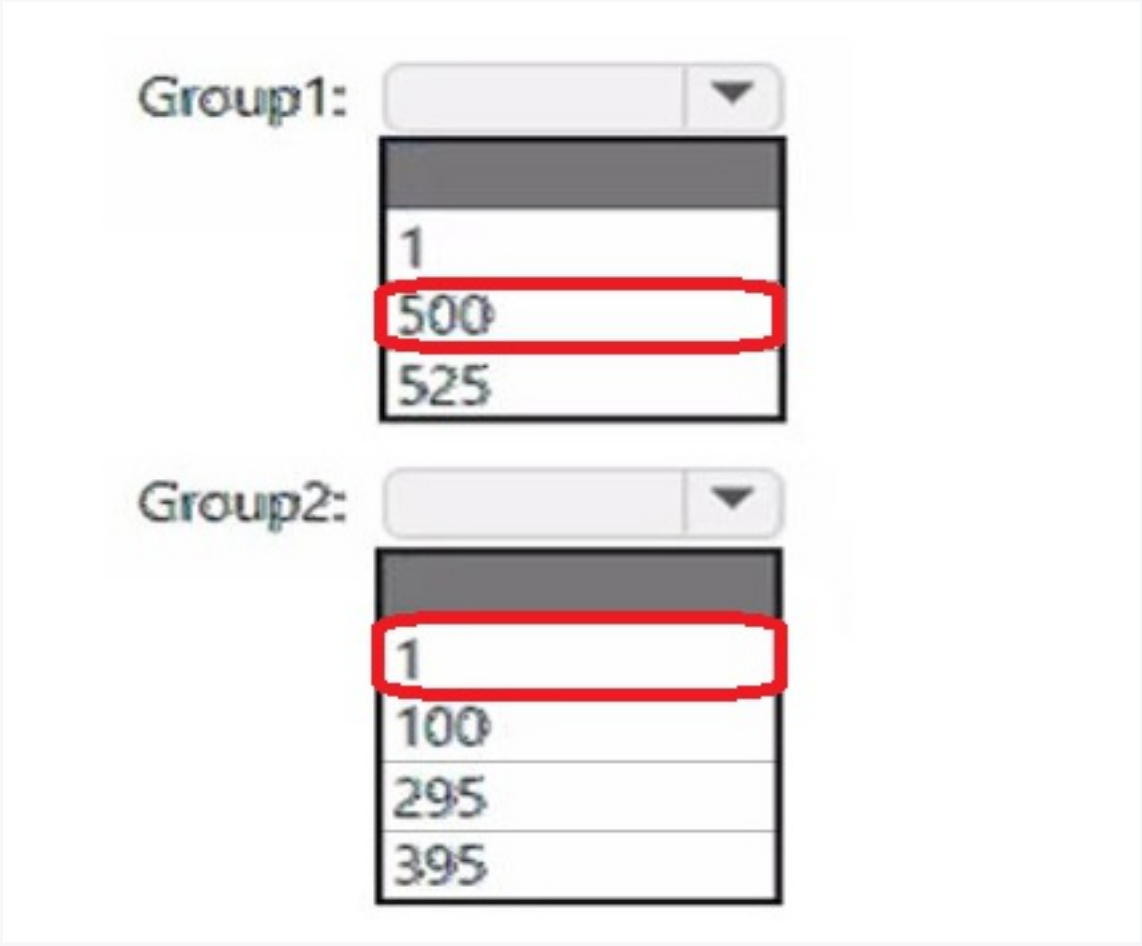
You create an access review for Group2 as shown in the following table.

Setting	Value
Review type	Teams + Groups
Review scope	Guest users only
Reviewers	Group owner

What is the minimum member of Azure Active Directory Premium P2 licenses required for each group? To answer, select the appropriate, options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:



Answer:



Explanation:

Box 1: 500

In your Azure AD tenant, guest user collaboration usage is billed based on the count of unique guest users with authentication activity within a calendar month. This model replaces the 1:5 ratio billing model, which allowed up to five guest users for each Azure AD Premium license in your tenant. When your tenant is linked to a subscription and you use External Identities features to collaborate with guest users, you'll be automatically billed using the MAU-based billing model.

Your first 50,000 MAUs per month are free for both Premium P1 and Premium P2 features. To determine the total number of MAUs, we combine MAUs from all your tenants (both Azure AD and Azure AD B2C) that are linked to the same subscription.

Box 2: 1 -

For Group2:

Review scope: Guest users only. Reviewers: Group Owner.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview#license-requirements

Question: 242 CertyIQ

HOTSPOT -
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains a group named All Company and has the following Identity Governance settings:
- Block external users from signing in to this directory: Yes
- Remove external user. Yes
- Number of days before removing external user from this directory: 30

On March 11, 2.022, you create an access package named Package1 that has the following settings:
- Resource rales

1. Name: All Company
2. Type: Group and Team
3. Role: Member

- Lifecycle

1. Access package assignment expire: On date
2. Assignment expiration date: April 1, 2022

On March 1, 2022, you assign Package1 to the guest users shown in the following table.

Name	Email address
Guest1	guest1@outlook.com
Guest2	guest2@outlook.com

On March 2, 2022, you assign the Reports reader role to Guest1.
On April 1, 2022, you invite a guest user named Guest3 to contoso.com.
On April 4, 2022, you add Guest3 to the All Company group.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:

Statements	Yes	No
On May 5, 2022, the Guest1 account is in contoso.com.	○	○
On May 5, 2022, the Guest2 account is in contoso.com.	○	○
On May 5, 2022, the Guest3 account is in contoso.com.	○	○

Answer:

Statements	Yes	No
On May 5, 2022, the Guest1 account is in contoso.com.	○	○
On May 5, 2022, the Guest2 account is in contoso.com.	○	○
On May 5, 2022, the Guest3 account is in contoso.com.	○	○

Explanation:
Box 1: No -
On March 2, 2022, you assign the Reports reader role to Guest1.
On April 1 the access package assignment expires. After another 30 days, well before May 5, the guest user account is removed.

Box 2: No -
On April 1 the access package assignment expires. After another 30 days, well before May 5, the guest user account is removed.

Box 3: Yes -

Note: Lifecycle -
On the Lifecycle tab, you specify when a user's assignment to the access package expires. You can also specify whether users can extend their assignments.
In the Expiration section, set Access package assignments expires to On date, Number of days, Number of hours, or Never.
For On date, select an expiration date in the future.
For Number of days, specify a number between 0 and 3660 days.
For Number of hours, specify a number of hours.
Based on your selection, a user's assignment to the access package expires on a certain date, a certain number of days after they are approved, or never.
Note 2: By default, when an external user no longer has any access package assignments, they are blocked from signing in to your directory. After 30 days, their guest user account is removed from your directory.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-lifecycle-policy https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-external-users

Question: 243 CertyIQ

You have an Azure Active Directory (Azure AD) tenant named Contoso that contains a terms of use (Toll) named Terms1 and an access package. Contoso users collaborate with an external organization named Fabrikam.
Fabrikam users must accept Terms1 before being allowed to use the access package.
You need to identify which users accepted or declined Terms1.
What should you use?

A. sign-in logs
B. the Usage and Insights report
C. provisioning logs
D. audit logs

Answer: D

Explanation:
View Azure AD audit logs -
If you want to view more activity, Azure AD terms of use policies include audit logs. Each user consent triggers an event in the audit logs that is stored for 30 days.
You can view these logs in the portal or download as a .csv file.
To get started with Azure AD audit logs, use the following procedure:
1. Sign in to the Azure portal as a global administrator, security administrator, or Conditional Access administrator.
2. Browse to Azure Active Directory > Security > Conditional Access > Terms of use.
3. Select a terms of use policy.
4. Select View audit logs.
5. On the Azure AD audit logs screen, you can filter the information using the provided lists to target specific audit log information.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use

Question: 244 CertyIQ

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

Name	User type	Member of
User1	Member	Group1
User2	Member	Group1
User3	Guest	Group1

User1 is the owner of Group1.
You create an access review that has the following settings:
- What to review: Teams + Groups
- Scope: All users
- Group: Group1
- Reviewers: Users review their own access

Which users can perform access reviews for User3?

A. User1 only
B. User3 only

C. User1 and User2 only

D. User1, User2, and User3

Answer: B

Explanation:

Correct answer is B: User3

You can ask the guests themselves or a decision maker to participate in an access review and recertify (or attest) to the guests' access.

Refer to the below article:

https://learn.microsoft.com/en-us/azure/active-directory/governance/manage-guest-access-with-access-reviews

Question: 245

CertyIQ

HOTSPOT -
You have an Azure Active Directory (Azure AD) tenant that contains three users named User1, User2, and User3.
You create a group named Group1. You add User2 and User3 to Group1.
You configure a role in Azure AD Privileged Identity Management (PIM) as shown in the Application Administrator exhibit. (Click the Application Administrator tab.)

Role setting details - Application Administrator

Privileged Identity Management | Azure AD roles

Edit

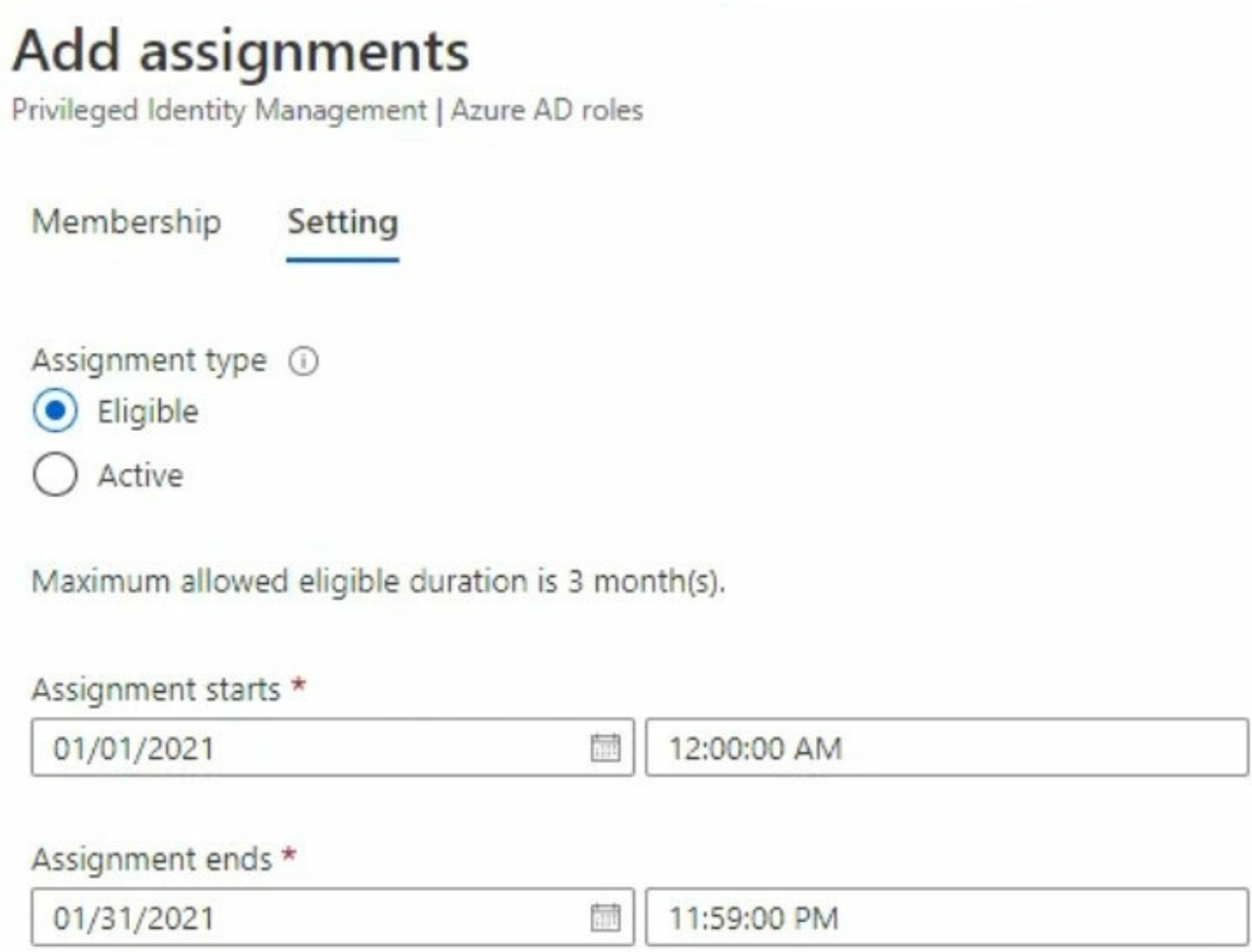
Activation

Setting	State
Activation maximum duration (hours)	5 hour(s)
Require justification on activation	Yes
Require ticket information on activation	No
Require approval to activate	Yes
Approvers	0 Member(s), 1 Group(

Assignment

Setting	State
Allow permanent eligible assignment	No
Expire eligible assignments after	3 month(s)
Allow permanent active assignment	No
Expire active assignments after	1 month(s)
Require Azure Multi-Factor Authentication on acti...	No
Require justification on active assignment	Yes

Group1 is configured as the approver for the Application administrator role.
You configure User2 to be eligible for the Application administrator role.
For User1 you add an assignment to the Application administrator role as shown in the Assignment exhibit. (Click the Assignment tab.)



For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:

Statements	Yes	No
User1 is assigned the Application administrator role automatically.	○	○
When User2 requests to be assigned the Application administrator role, only User3 can approve the request.	○	○
If a request by User1 to be assigned the Application administrator role is approved on January 31, 2021, at 23:00, User1 can use the role until February 1, 2021, at 04:00.	○	○

Answer:

Statements	Yes	No
User1 is assigned the Application administrator role automatically.	○	○
When User2 requests to be assigned the Application administrator role, only User3 can approve the request.	○	○
If a request by User1 to be assigned the Application administrator role is approved on January 31, 2021, at 23:00, User1 can use the role until February 1, 2021, at 04:00.	○	○

Explanation:

Box 1: No -

User1 is eligible from 1/1/2021 to 1/31/2021.

However, here the Application Administrator role requires approval.

Box 2: Yes-

you cannot approve a request for yourself. Also, if there are guest accounts in the group, they will receive the email about approving the request but they cannot do it

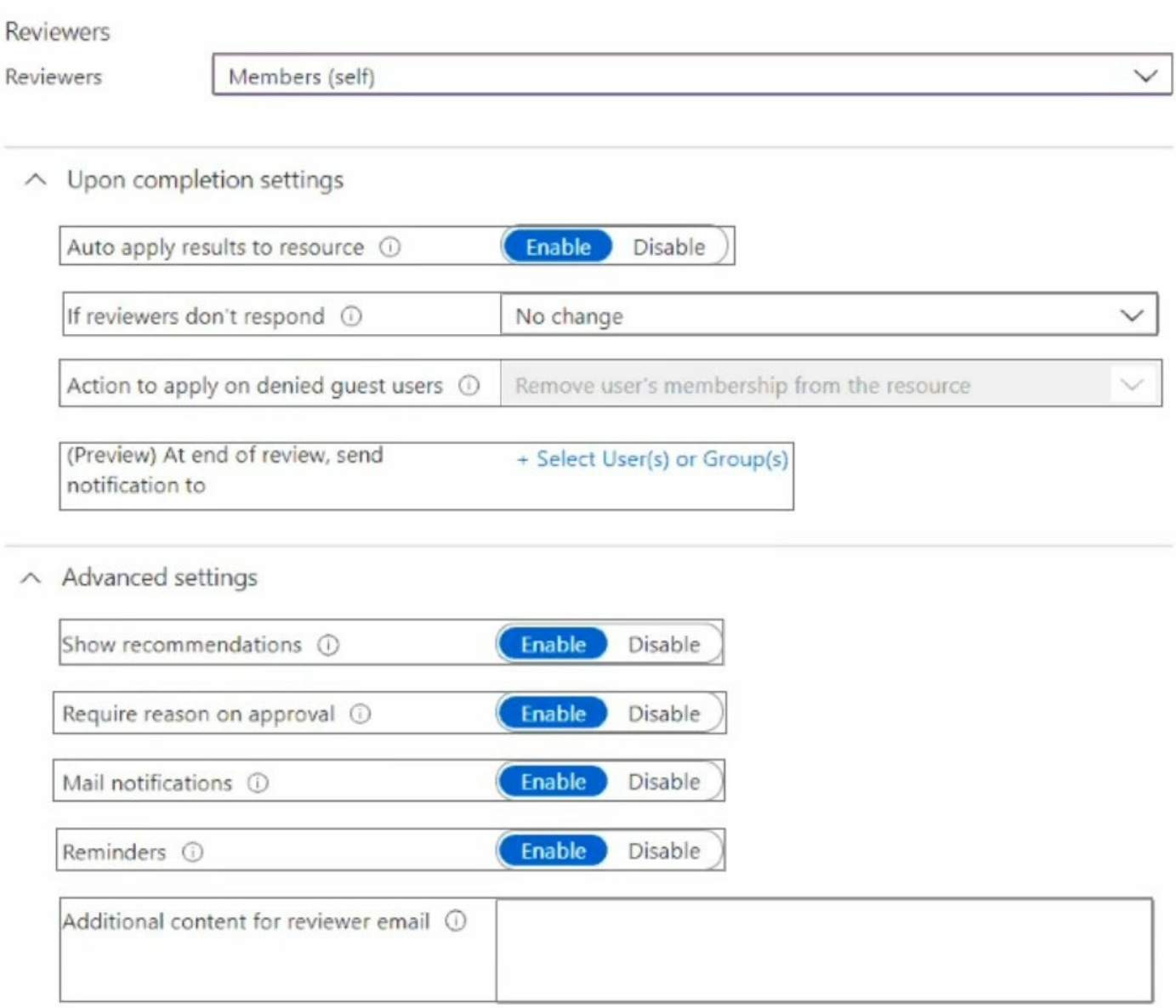
Box 3: Yes -

User1 is eligible from 1/1/2021 to 1/31/2021.

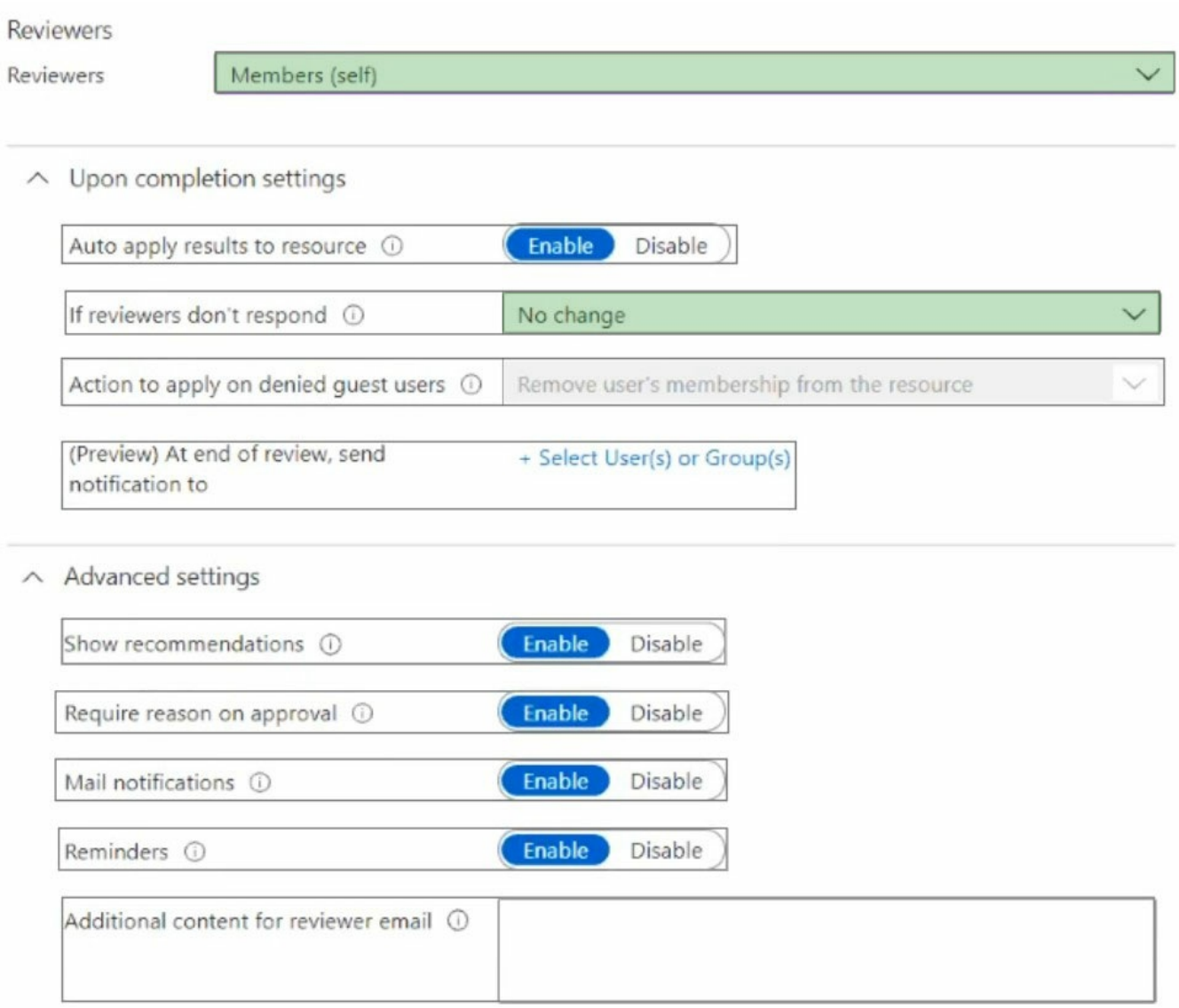
Activation maximum duration (hours) is set to 5 hours.

Question: 246 CertyIQ

HOTSPOT -
You have a Microsoft 365 E5 subscription.
You create an access review for Azure Active Directory (Azure AD) roles.
You need to ensure that users who do not respond to review requests are removed automatically from the roles.
The solution must minimize administrative effort.
Which two settings should you modify? To answer, select the settings in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:


Reviewers
Reviewers
Members (self)
Upon completion settings
Auto apply results to resource
Enable
Disable
If reviewers don't respond
No change
Action to apply on denied guest users
Remove user's membership from the resource
(Preview) At end of review, send notification to
+ Select User(s) or Group(s)
Advanced settings
Show recommendations
Enable
Disable
Require reason on approval
Enable
Disable
Mail notifications
Enable
Disable
Reminders
Enable
Disable
Additional content for reviewer email

Answer:



Explanation:
Box 1: Reviewers, Members (self)
Reviewers for guest users can be:
Specified reviewers: Certain users within your organization
Group owners: Office 365 Group owners that also includes Teams
Self-review: Guest users can review access on their own
Box 2: If reviewers don't respond, No Change
If reviewers don't respond (within the configured review period):
No change: Leave user's access unchanged
Remove access: Remove user's access
Approve access: Approve user's access
Take recommendations: Take the system's recommendation on denying or approving the user's continued access

Reference:
https://blog.quadrotech-it.com/blog/how-to-manage-guest-access-in-azure-active-directory-pt-1/

Question: 247 CertyIQ

HOTSPOT
-

You have an Azure Active Directory (Azure AD) tenant that contains a user named User1.

An administrator deletes User1.

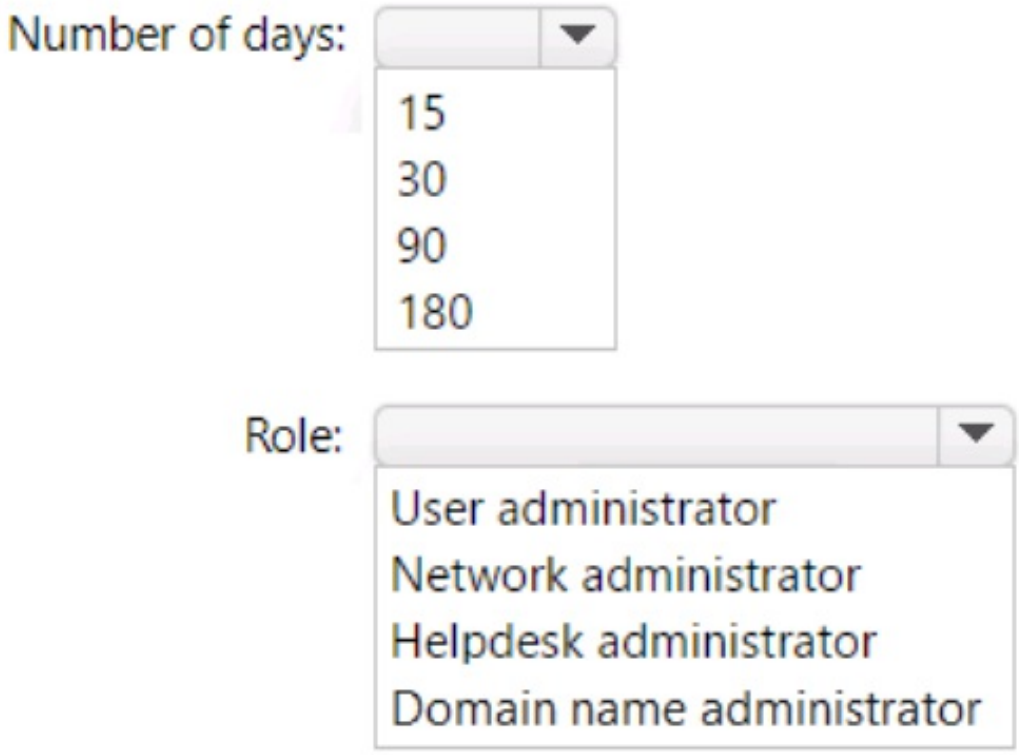
You need to identify the following:

• How many days after the account of User1 is deleted can you restore the account?
• Which is the least privileged role that can be used to restore User1?

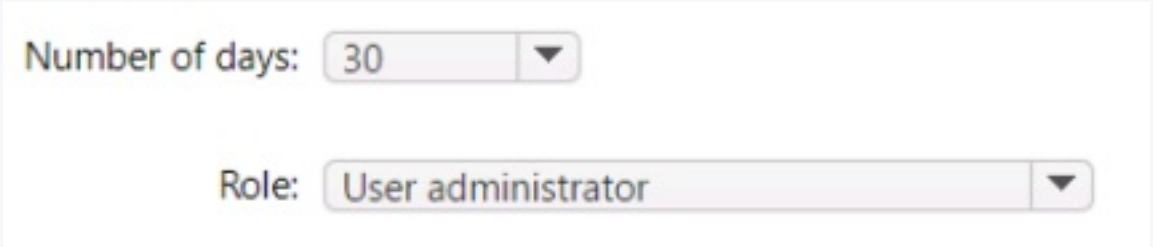
What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



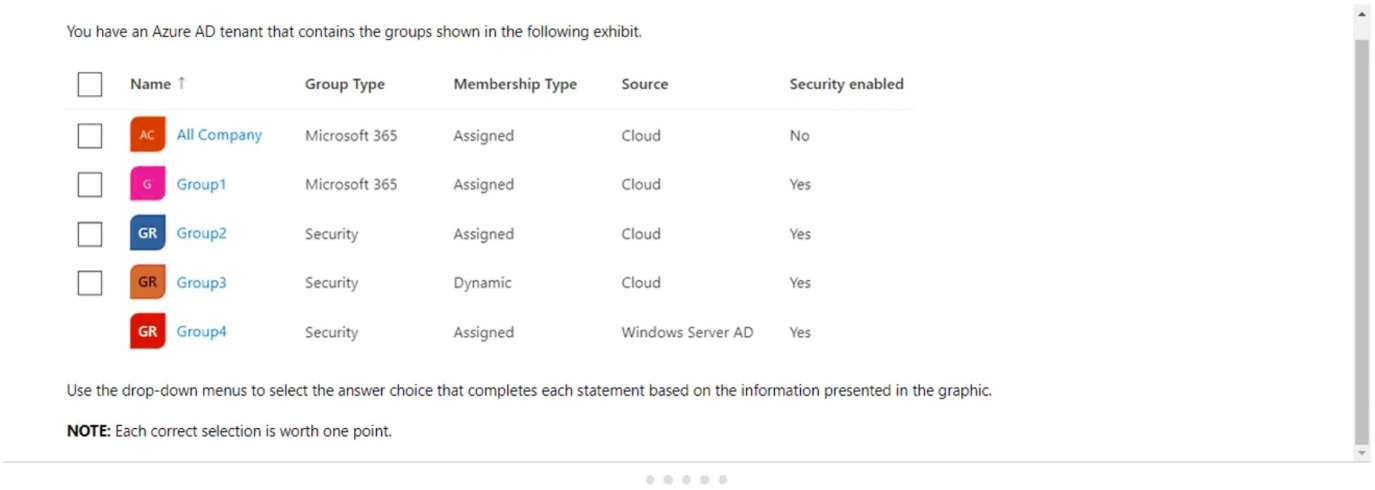
Answer:



Question: 248 CertyIQ

HOTSPOT
-

You have an Azure AD tenant that contains the groups shown in the following exhibit.



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

NOTE: Each correct selection is worth one point.

Answer Area

You can add a managed identity to **<answer choice>**.

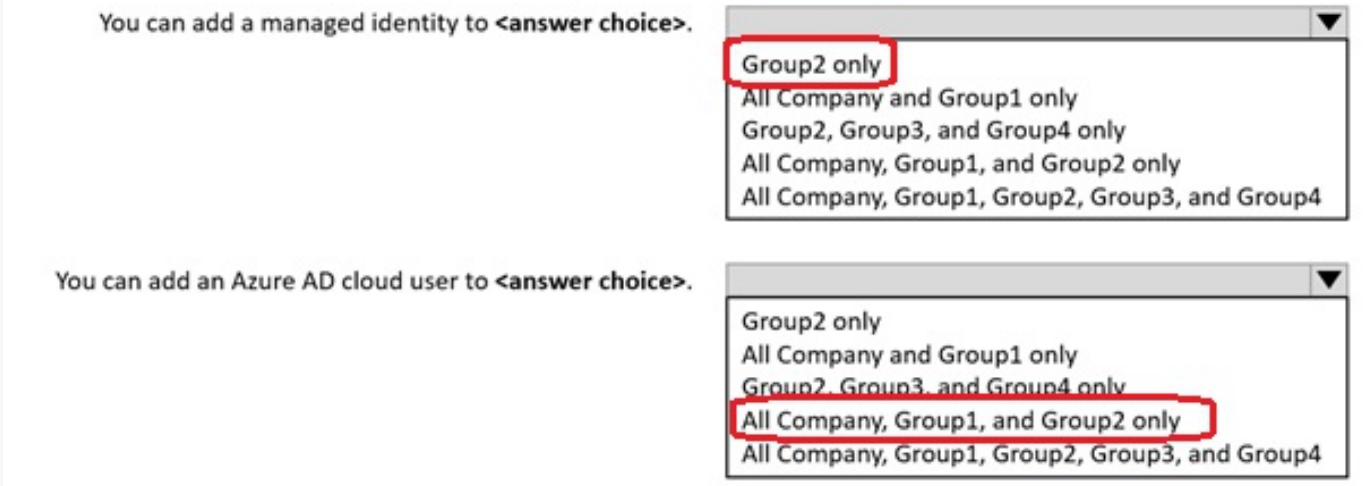
- Group2 only
- All Company and Group1 only
- Group2, Group3, and Group4 only
- All Company, Group1, and Group2 only
- All Company, Group1, Group2, Group3, and Group4

You can add an Azure AD cloud user to **<answer choice>**.

- Group2 only
- All Company and Group1 only
- Group2, Group3, and Group4 only
- All Company, Group1, and Group2 only
- All Company, Group1, Group2, Group3, and Group4

Answer:

Answer Area



Explanation:

- Managed identity to Security group only.

The security group can't be Dynamic or sync from OnPremise

- AD User Cloud can be added to Security and M365 groups

○ Not the dynamic (Group3) as it's using a query to get members

Not Group4 as it's synch from OnPrem

Question: 249

CertyIQ

You have an Azure AD tenant that contains two users named User1 and User2.

You plan to perform the following actions:

• Create a group named Group1.
• Add User1 and User2 to Group1.
• Assign Azure AD roles to Group1.

You need to create Group1.

Which two settings can you use? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Group type: Microsoft 365 -
Membership type: Assigned

B. Group type: Security -
Membership type: Assigned

C. Group type: Security -
Membership type: Dynamic User

D. Group type: Microsoft 365 -
Membership type: Dynamic User

E. Group type: Security -
Membership type: Dynamic Device

Answer: AB

Explanation:

when you create a group you MUST enable "azure ad roles can be assigned to the group" (cannot be done afterwards). If you enable this feature when creating a group, dynamic groups are getting greyed out / disabled.

Question: 250

CertyIQ

DRAG DROP
-

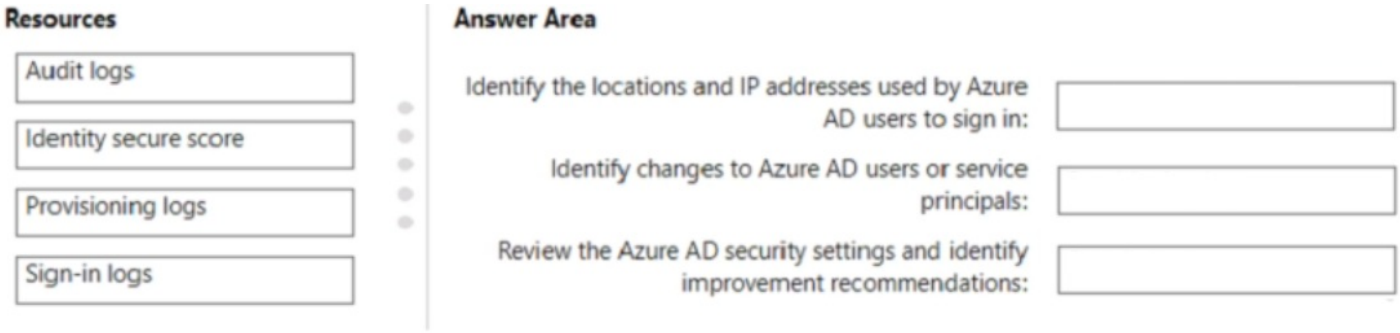
You have a Microsoft 365 E5 subscription.

You need to perform the following tasks:

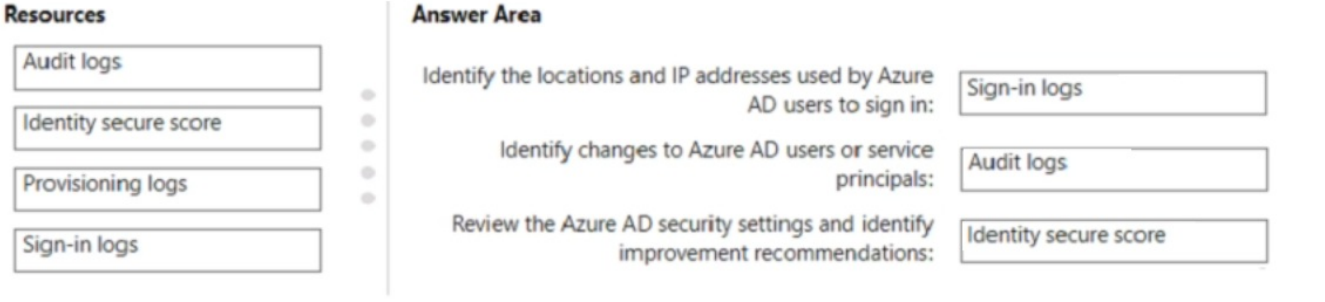
• Identify the locations and IP addresses used by Azure AD users to sign in.
• Review the Azure AD security settings and identify improvement recommendations.
• Identify changes to Azure AD users or service principals.

What should you use for each task? To answer, drag the appropriate resources to the correct requirements. Each resource may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



Answer:



Question: 251

CertyIQ

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 Package1.

Which users can create and manage the access review?

A.User3 only
B.User4 only
C.User5 only
D.User3 and User4
E.User3 and User5
F.User4 and User5

Answer: E

Explanation:

First, you must be assigned one of the following roles: Global administrator User administrator Identity Governance Administrator Privileged Role Administrator (for reviews of role-assignable groups only)(Preview) Microsoft 365 or AAD Security Group owner of the group to be reviewedhttps://learn.microsoft.com/en-us/azure/active-directory/governance/manage-access-review

Question: 252 CertyIQ

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 guest user invitations.

What should you do for the Azure AD tenant?

A.Configure the Continuous access evaluation settings.

B.Configure a Conditional Access policy.

C.Modify the External collaboration settings.

D.Configure the Access reviews settings.

Answer: C

Explanation:

Azure Portal > Azure AD > External identities > External collaboration settings > (Guest invite settings Section) check "Only users assigned to specific admin roles can invite guest users"

Question: 253

CertyIQ

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 modify the settings of the User administrator role to meet the technical requirements.

Which two actions should you perform for the role? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A.Select Require justification on activation.
B.Select Require ticket information on activation.
C.Modify the Expire eligible assignments after setting.
D.Set all assignments to Eligible.
E.Set all assignments to Active.

Answer: CD

Explanation:

C.Modify the Expire eligible assignments after setting.

D.Set all assignments to Eligible.

Question: 254 CertyIQ

You have a Microsoft 365 E5 subscription that contains a user named User1.

You need to ensure that User1 can create access reviews for Azure AD roles. The solution must use the principle of least privilege.

Which role should you assign to User1?

A.Privileged role administrator
B.Identity Governance Administrator
C.User administrator

D.User Access Administrator

Answer: A

Explanation:
1. To create access reviews for Azure resources, you must be assigned to the Owner or the User Access Administrator role for the Azure resources. To create access reviews for Azure AD roles, you must be assigned to the Global Administrator or the Privileged Role Administrator role.https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-create-roles-and-resource-roles-review#prerequisites
2. To create access reviews for Azure resources, you must be assigned to the Owner or the User Access Administrator role for the Azure resources. To create access reviews for Azure AD roles, you must be assigned to the Global Administrator or the Privileged Role Administrator role.

Question: 255 CertyIQ

HOTSPOT
-

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

You have two Azure AD roles that have the Activation settings shown in the following table.

Name	Required justification on activation	Require approval to activate	Approvers
Role1	No	Yes	User1
Role2	Yes	No	None

The Azure AD roles have the Assignment settings shown in the following table.

Role	Allow permanent eligible assignment	Allow Permanent activate assignment	Require justification on active assignment
Role1	Yes	Yes	Yes
Role2	No	Yes	Yes

The Azure AD roles have the eligible users shown in the following table.

Role	Eligible assignment
Role1	User1, User2
Role2	User3

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
If User1 requests Role1, the request will be approved automatically.	○	○
User1 can approve the request of User3 for Role2.	○	○
User1 must provide justification to approve the request of User2 for Role1.	○	○

Answer:

Answer Area

Statements	Yes	No
If User1 requests Role1, the request will be approved automatically.	○	○
User1 can approve the request of User3 for Role2.	○	○
User1 must provide justification to approve the request of User2 for Role1.	○	○

Explanation:

N, N, Y. . Require justification on active assignment is Yes for Role 1.

https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-resource-roles-configure-role-settings#require-justification-on-active-assignment

Question: 256

CertyIQ

HOTSPOT
-

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

Name	Role
Admin1	Global Administrator
Admin2	Application Administrator
Admin3	Cloud Application Administrator
Admin4	Application Developer
User1	*None*

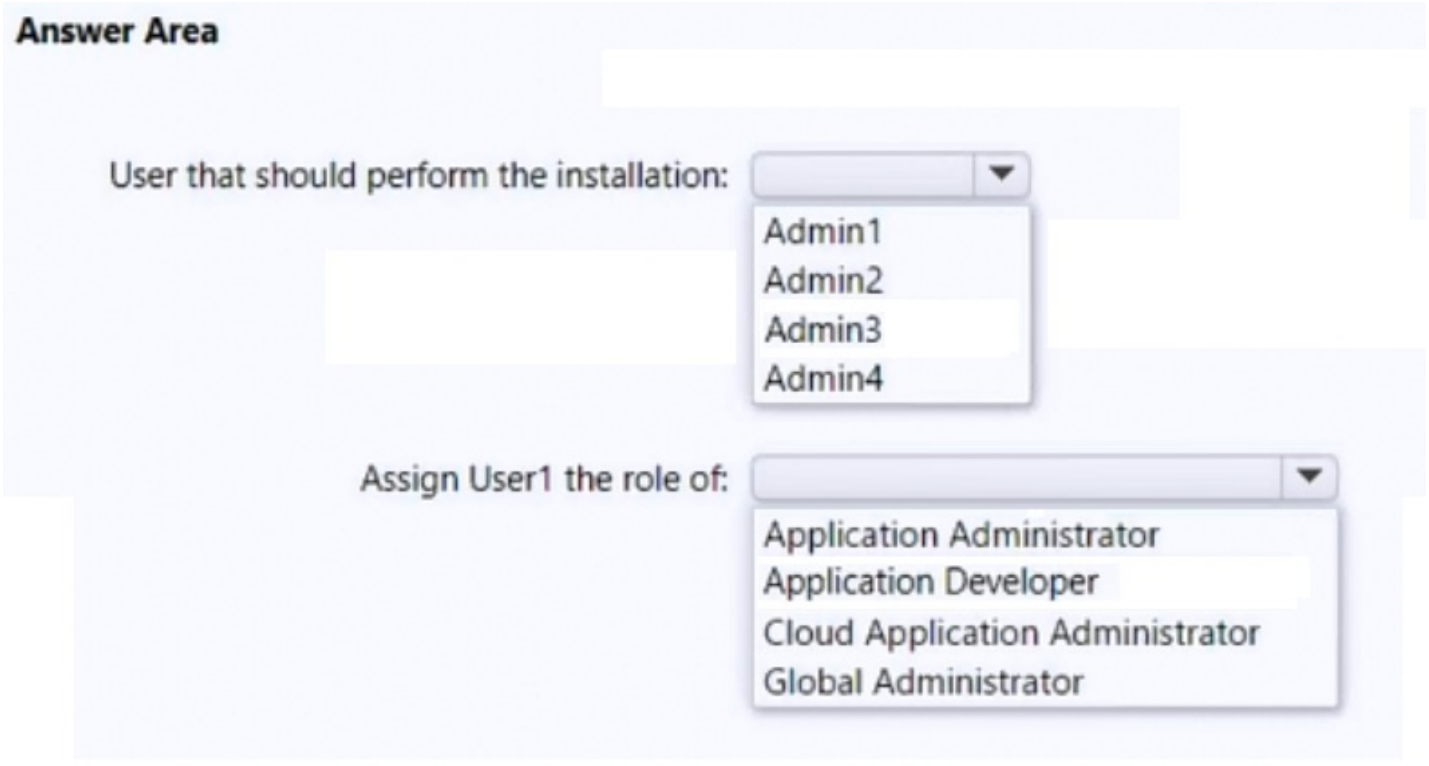
You plan to deploy an on-premises app named App1. App1 will be registered in Azure AD and will use Azure AD Application Proxy.

You need to delegate the installation of the Application Proxy connector and ensure that User1 can register App1 in Azure AD. The solution must use the principle of least privilege.

Which user should perform the installation, and which role should you assign to User1? To answer, select the appropriate options in the answer area.

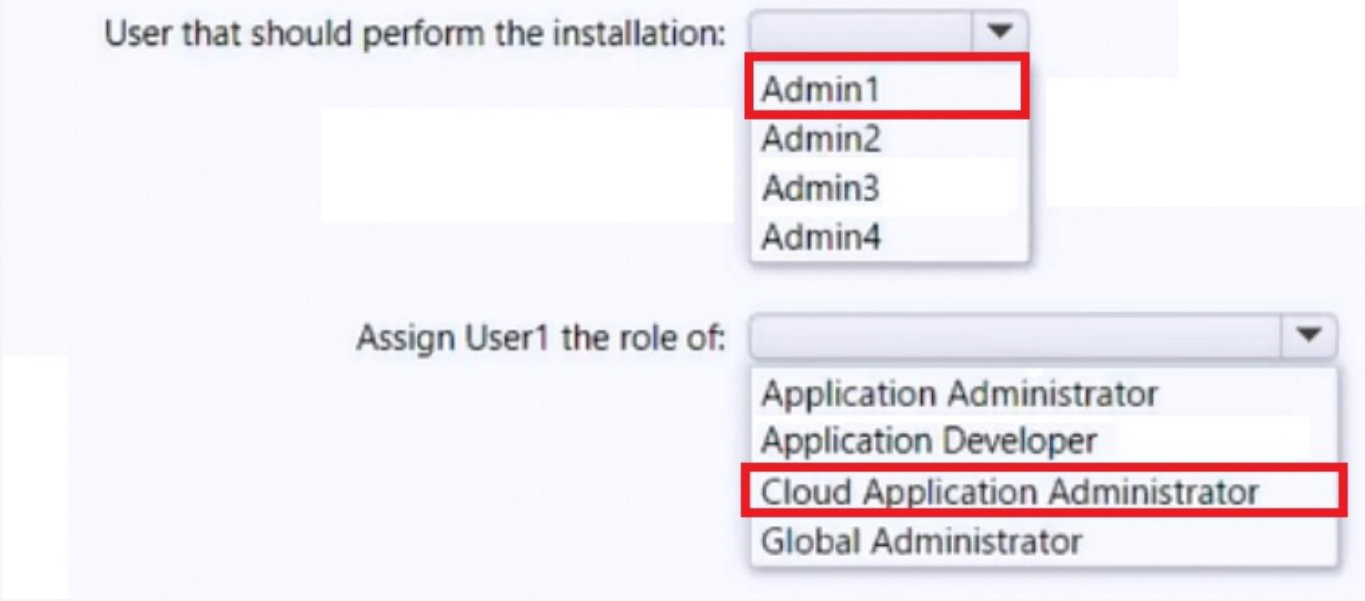
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area



Explanation:

Admin 1

Cloud Application Administrator

Question: 257 CertyIQ

HOTSPOT
-

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

Name	Member of administrative unit
User1	AU1
User2	AU1
User3	AU1
User4	AU2
User5	Not a member of an administrative unit

The users are assigned the roles shown in the following table.

User	Role	Role scope
User1	Password Administrator	Organization
User2	Global Reader	Organization
User3	*None*	*Not applicable*
User4	Password Administrator	AU1
User5	*None*	*Not applicable*

For which users can User1 and User4 reset passwords? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

User 1:

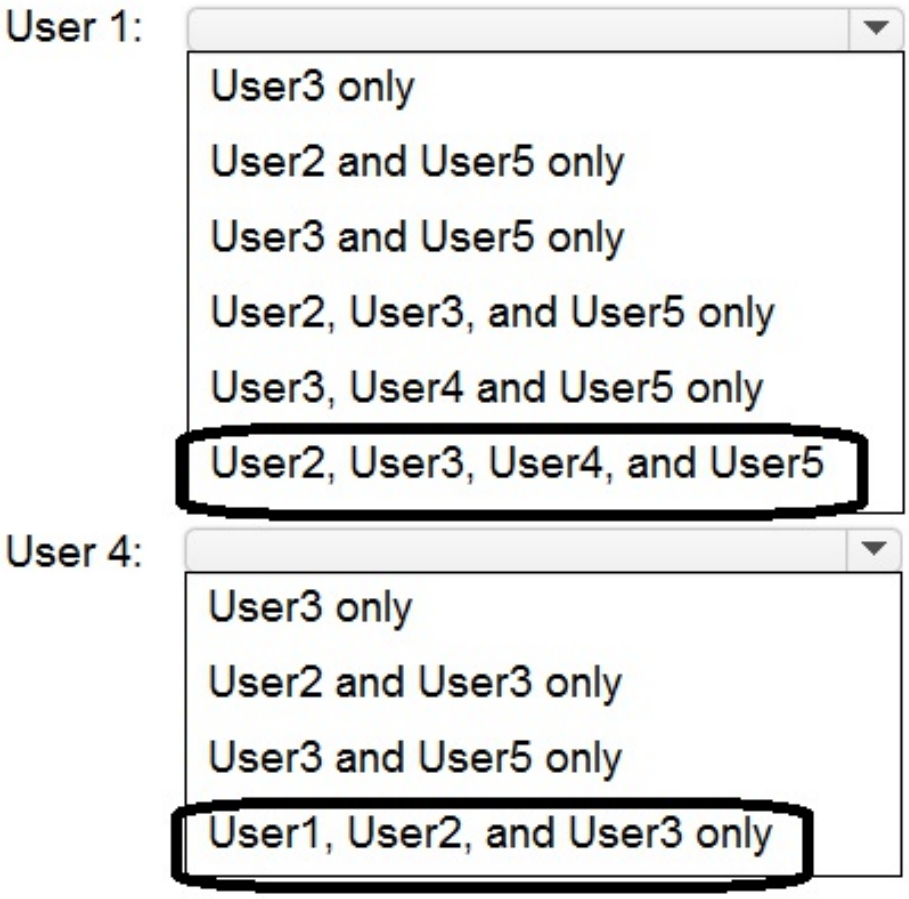
- User3 only
- User2 and User5 only
- User3 and User5 only
- User2, User3, and User5 only
- User3, User4 and User5 only
- User2, User3, User4, and User5

User 4:

- User3 only
- User2 and User3 only
- User3 and User5 only
- User1, User2, and User3 only

Answer:

Answer Area



Explanation:

User1 -> User2, User3, User4, User5

User4 -> User1, User2 & User3 on;y

Can reset passwords for non-administrators and Password Administrators

https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#who-can-reset-passwords

Question: 258 CertyIQ

You have a Microsoft 365 E5 subscription that contains a user named User1. User is eligible for the Application administrator role.

User1 needs to configure a new connector group for an application proxy.

What should you use to activate the role for User1?

A.the Microsoft Defender for Cloud Apps portal
B.the Microsoft 365 admin center
C.the Azure Active Directory admin center
D.the Microsoft 365 Defender portal

Answer: C

Explanation:

https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-activate-role

Question: 259 CertyIQ

You have an Azure subscription that contains a registered app named App1.

You need to review the sign-in activity for App1. The solution must meet the following requirements:

•Identify the number of failed sign-ins.
•Identify the success rate of sign-ins.
•Minimize administrative effort.

What should you use?

A.Sign-in logs
B.Access reviews
C.Audit logs
D.Usage & insights

Answer: D

Explanation:
1. D: Usage & insights

Question: 260 CertyIQ

Your company has an Azure AD tenant that contains a user named User1.

The company has two departments named marketing and finance.

You need to grant permissions to User1 to manage only the users in the marketing department. The solution must ensure that User1 does NOT have permissions to manage the users in the finance department.

What should you create first?

A.a management group
B.an administrative unit
C.a resource group
D.a Microsoft 365 group

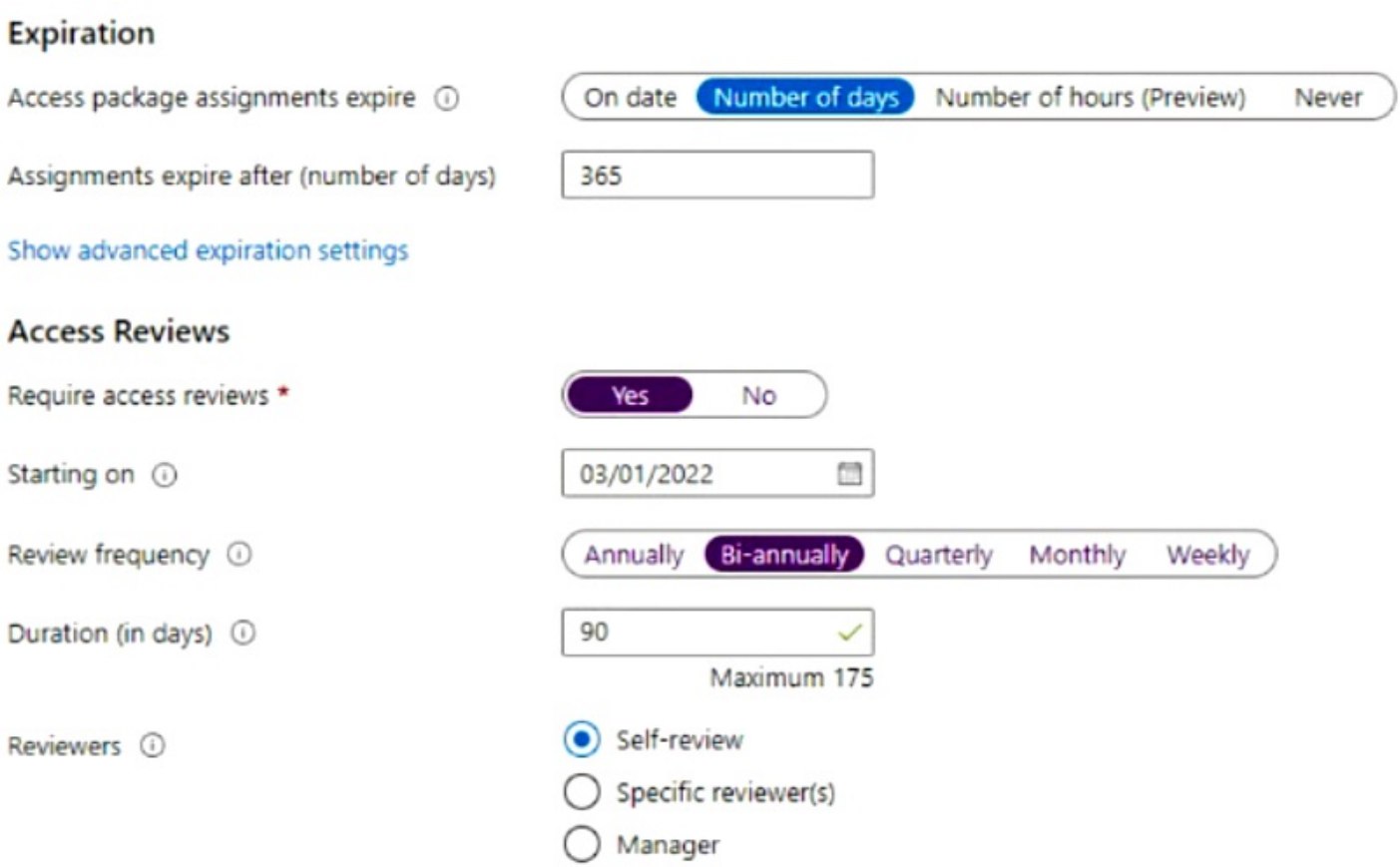
Answer: B

Explanation:

B. an administrative unit

Question: 261 CertyIQ

You have an Azure AD tenant that contains an access package named Package1 and a user named User1. Package1 is configured as shown in the following exhibit.



You need to ensure that User1 can modify the review frequency of Package1. The solution must use the principle of least privilege.

Which role should you assign to User1?

A.Security administrator
B.Privileged role administrator
C.External Identity Provider administrator
D.User administrator

Answer: D

Explanation:

o enable reviews of access packages, you must meet the prerequisites for creating an access package:Microsoft Azure AD Premium P2 or Microsoft Entra ID GovernanceGlobal administrator, Identity Governance administrator, User administrator, Catalog owner, or Access package manager

Question: 262

CertyIQ

HOTSPOT
-

You have an Azure subscription.

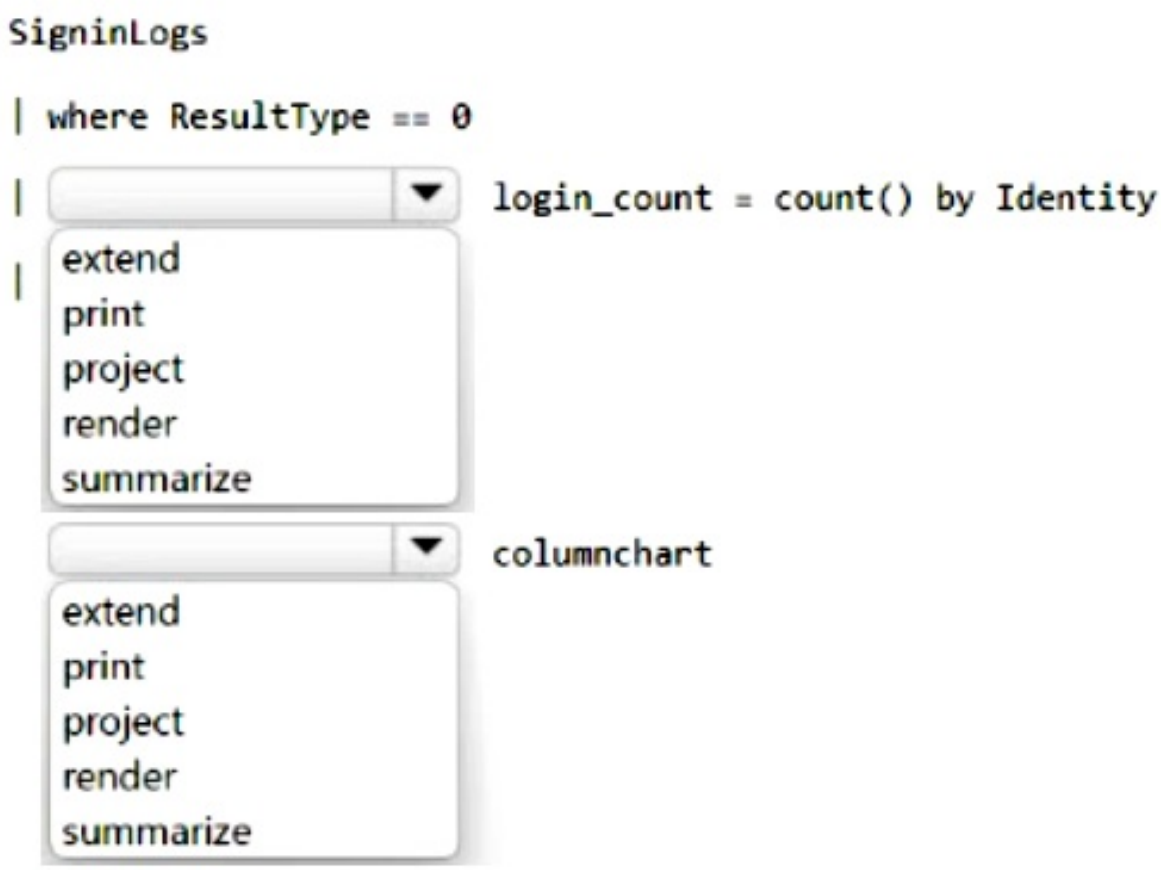
Azure AD logs are sent to a Log Analytics workspace.

You need to query the logs and graphically display the number of sign-ins per user.

How should you complete the query? To answer, select the appropriate options in the answer area,

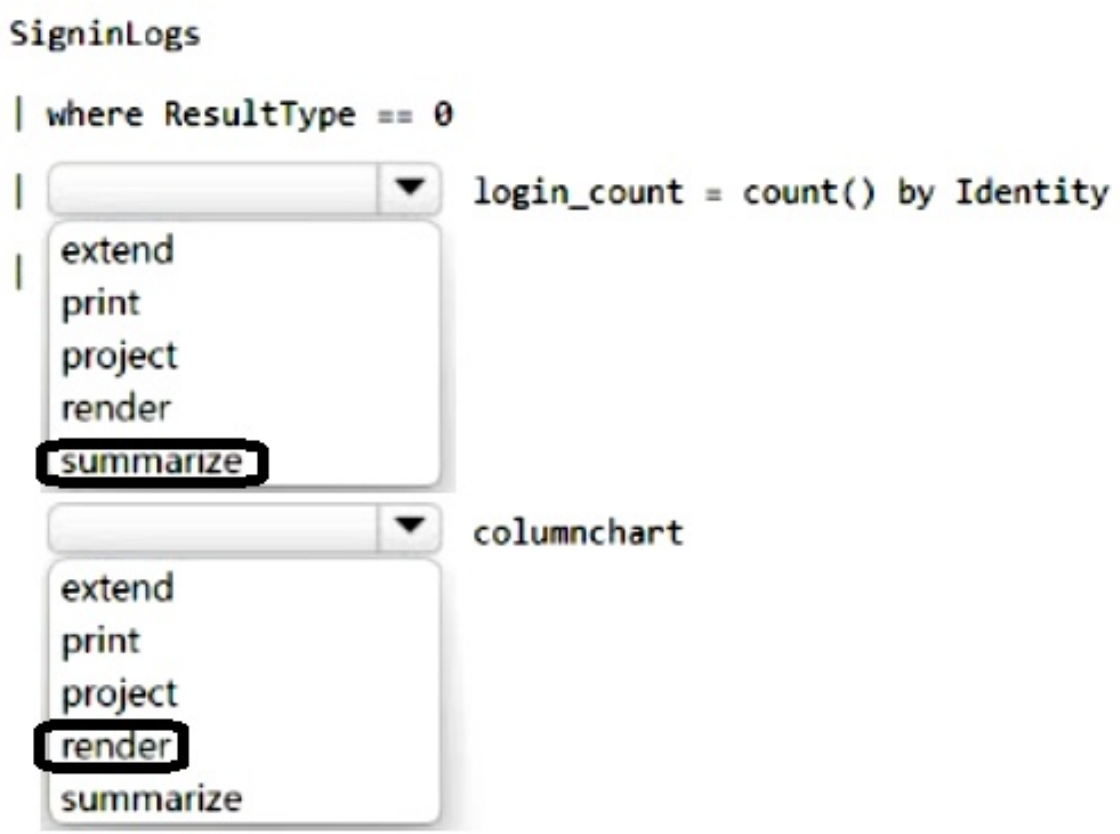
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area



Explanation:

Sign in Logs |where Result Type == 0|summarize login_ count = count() by Identity| render column chart.

Question: 263 CertyIQ

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

You need to identify which users access Facebook from their devices and browsers. The solution must minimize administrative effort.

What should you do first?

A.Create a Conditional Access policy.
B.Create a Defender for Cloud Apps access policy.
C.Create an app configuration policy in Microsoft Endpoint Manager.
D.From the Microsoft Defender for Cloud Apps portal, unsanction Facebook.

Answer: D

Explanation:

Unsanctioning an app doesn't block use, but enables you to more easily monitor its use with the Cloud Discovery filters. You can then notify users of the unsanctioned app and suggest an alternative safe app for their use, or generate a block script using the Defender for Cloud Apps APIs to block all unsanctioned apps.

https://learn.microsoft.com/en-us/defender-cloud-apps/governance-discovery#sanctioningunsanctioning-an-app

Question: 264 CertyIQ

You have an Azure subscription that uses Azure AD Privileged Identity Management (PIM).

You need to identify users that are eligible for the Cloud Application Administrator role.

Which blade in the Privileged Identity Management settings should you use?

A.Azure resources
B.Privileged access groups
C.Review access
D.Azure AD roles

Answer: D

Explanation:
1. A. Role does not fitB. Blade does not existC. Makes sense only if an access review would existD: Easiest way: Azure AD roles -> AssignmentsAny other suggestions?

Question: 265 CertyIQ

HOTSPOT
-

You have a Microsoft 365 E5 subscription.

You need to create a dynamic user group that will include all the users that do NOT have a department defined in their user profile.

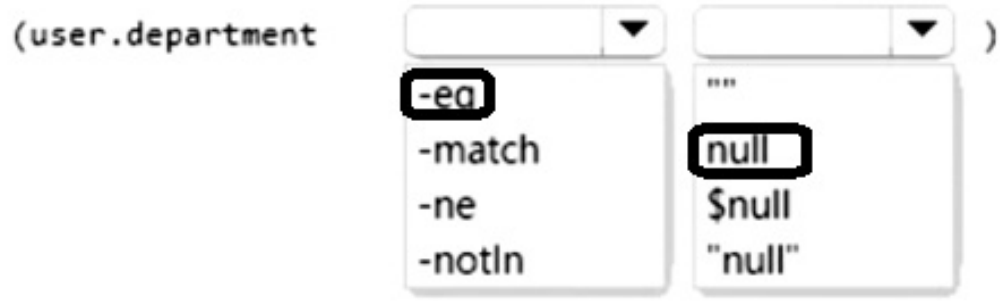
How should you complete the membership rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Answer Area



Explanation:

(user.department -eq null

)https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership#use-of-null-values

Question: 266 CertyIQ

You have an Azure AD Premium P2 tenant.

You create a Log Analytics workspace.

You need to ensure that you can view Azure AD audit log information by using Azure Monitor.

What should you do first?

A.Modify the Diagnostics settings for Azure AD.
B.Run the Update-MgOrganization cmdlet.
C.Run the Update-MgDomain cmdlet.
D.Create an Azure AD workbook.

Answer: A

Explanation:

A. Modify the Diagnostics settings for Azure AD.

Question: 267 CertyIQ

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

You need to identify which users access Facebook from their devices and browsers. The solution must minimize administrative effort.

What should you do first?

A.From the Microsoft 365 Defender portal, unsanction Facebook.
B.Create a Defender for Cloud Apps access policy.

C.Create an app configuration policy in Microsoft Intune.

D.Create a Conditional Access policy.

Answer: A

Explanation:

From the Microsoft 365 Defender portal, unsanction Facebook.

Question: 268 CertyIQ

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

Name	Role
User1	Global Administrator
User2	User Administrator
User3	Groups Administrator
User4	*None*

From the tenant, you configure a naming policy for groups.

Which users are affected by the naming policy?

A.User2 only

B.User3only

C.User2 and User3 only

D.User3 and User4 only

E.User1, User2, and User3 only

F.User1, User2, User3, and User4

Answer: D

Explanation:

Correct answer is D:.User3 and User4 only.

Question: 269 CertyIQ

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

Name	Role
Admin1	Account Administrator
Admin2	Service Administrator
Admin3	SharePoint Administrator

You need to implement Azure AD Privileged Identity Management (PIM).

Which users can use PIM to activate their role permissions?

A.Admin1 only
B.Admin2 only
C.Admin3 only
D.Admin1 and Admin2 only
E.Admin2 and Admin3 only
F.Admin1, Admin2, and Admin3

Answer: C

Explanation:

Classic subscription administrator rolesYou cannot manage the following classic subscription administrator roles in Privileged Identity Management:Account AdministratorService AdministratorCo-Administrator

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

Question: 270

CertyIQ

HOTSPOT
-

You have an Azure AD tenant.

You perform the tasks shown in the following table.

Date	Task
March 1	Register four enterprise applications named App1, App2, App3, and App4.
March 15	From the tenant, update the following settings for App1: App roles, Users and groups, Client secret, and Self-service.
March 20	From the tenant, update the following settings for App2: App roles, Users and groups, Client secret, and Self-service.
March 25	From the tenant, update the following settings for App3: App roles, Users and groups, Client secret, and Self-service.
March 30	From the tenant, update the following settings for App4: App roles, Users and groups, Client secret, and Self-service.

On April 5, an administrator deletes App1, App2, App3, and App4.

You need to restore the apps and the settings.

Which apps can you restore on April 16, and which settings can you restore for App4 on April 16? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

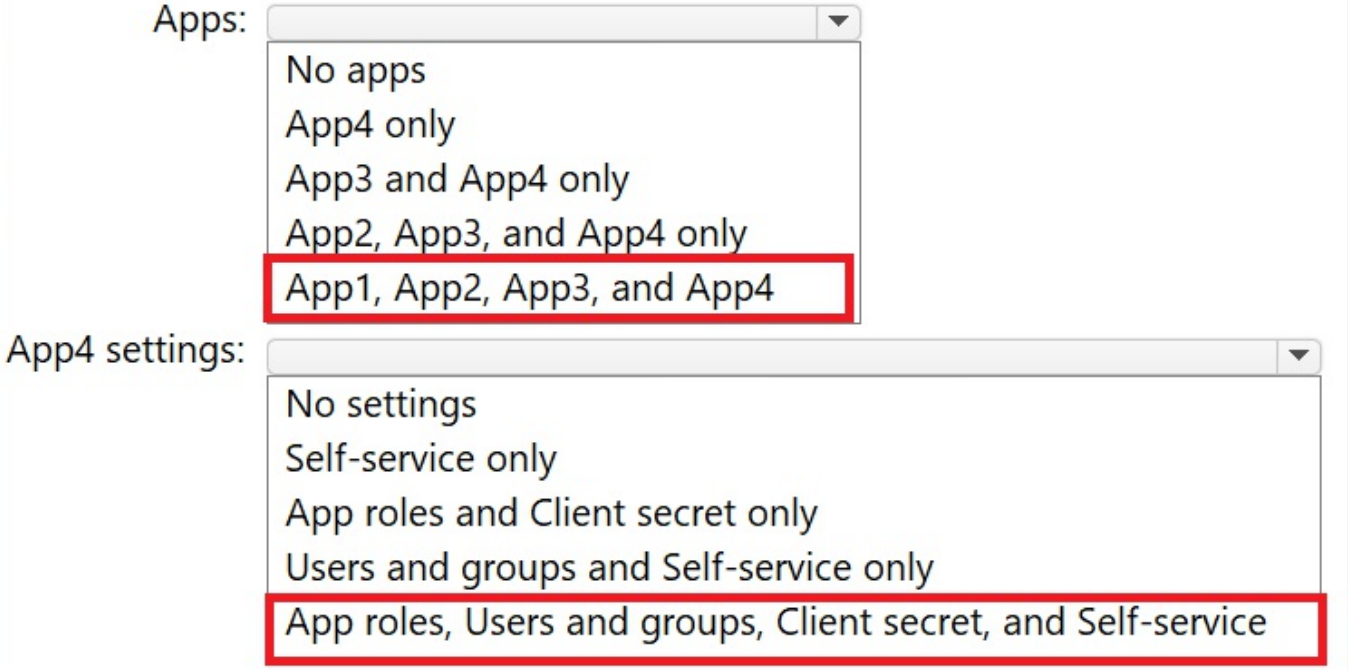
Answer Area

Apps:
- No apps
- App4 only
- App3 and App4 only
- App2, App3, and App4 only
- App1, App2, App3, and App4

App4 settings:
- No settings
- Self-service only
- App roles and Client secret only
- Users and groups and Self-service only
- App roles, Users and groups, Client secret, and Self-service

Answer:

Answer Area



Explanation:

Box 1: App1, App2, App3, and App4.

Box 2: App roles, Users and groups, client secret, and Self-service.

https://learn.microsoft.com/en-us/entra/identity-platform/howto-restore-app

Question: 271 CertyIQ

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

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

You have an Amazon Web Services (AWS) account, a Google Workspace subscription, and a GitHub account.

You deploy an Azure subscription and enable Microsoft 365 Defender.

You need to ensure that you can monitor OAuth authentication requests by using Microsoft Defender for Cloud Apps.

Solution: From the Microsoft 365 Defender portal, you add the GitHub app connector.

Does this meet the goal?

A.Yes

B.No

Answer: B

Explanation:

No, the solution does not meet the goal. Adding the GitHub app connector to Microsoft Defender for Cloud

Apps will allow you to monitor OAuth authentication requests from GitHub to Microsoft 365. However, it will not allow you to monitor OAuth authentication requests to your AWS account, Google Workspace subscription, or Azure subscription.

Question: 272 CertyIQ

You have an Azure AD tenant.

You plan to implement Azure AD Privileged Identity Management (PIM).

Which roles can you manage by using PIM?

A.Global Administrator only
B.Global Administrator and Security Administrator only
C.Global Administrator, Security Administrator, and Security Contributor only
D.Account Administrator, Global Administrator, Security Administrator, and Security Contributor only

Answer: C

Explanation:

The correct answer is C. Global Administrator, Security Administrator, and Security Contributor only.Azure AD Privileged Identity Management (PIM) can be used to manage the following roles:Global AdministratorSecurity AdministratorSecurity ContributorAccount AdministratorPrivileged Role AdministratorIdentity Governance AdministratorOther roles, such as User Administrator and Application Administrator, cannot be managed by using PIM.

Question: 273 CertyIQ

You have a Microsoft 365 tenant.

In Microsoft Entra ID, you configure the terms of use.

You need to ensure that only users who accept the terms of use can access the resources in the tenant. Other users must be denied access.

What should you configure?

A.Terms and conditions in Microsoft Intune
B.an access policy in Microsoft Defender for Cloud Apps
C.a conditional access policy in Microsoft Entra ID
D.a compliance policy in Microsoft Intune

Answer: C

Explanation:

C. a conditional access policy in Microsoft Entra ID. A conditional access policy is a feature that allows you to enforce granular controls over access to cloud apps based on user, location, device, and app. You can use a conditional access policy along with terms of use to require users to accept the terms of use policy before getting access to the resources in the tenant. You can also designate reviewers who can view and act on the consent requests in the Microsoft 365 admin center.

Question: 274 CertyIQ

You have a Microsoft 365 E5 subscription that contains a user named User1. User1 is eligible for the Application Administrator role.

User1 needs to configure a new connector group for an application proxy.

What should you use to activate the role for User1?

A.the Microsoft 365 Defender portal
B.the Microsoft 365 admin center
C.the Microsoft Intune admin center
D.the Azure Active Directory admin center

Answer: D

Explanation:

D. the Azure Active Directory admin center. The Azure Active Directory admin center is a portal that allows you to manage your Microsoft Entra ID resources, such as users, groups, roles, and applications. You can use the Azure Active Directory admin center to assign roles to users, either directly or through eligible assignments.

Question: 275 CertyIQ

Your on-premises network contains an Active Directory Domain Services (AD DS) domain and a certification authority (CA) named CA1.

You have an Azure AD tenant.

You need to implement certificate-based authentication in Azure AD. The solution must ensure that users can sign in by using certificates issued by CA1. What should you do first?

A.Deploy an Azure key vault.
B.Add CA1 as a Certificate Authority to the Microsoft Entra ID tenant.
C.Enable auto-enrollment for CA1.
D.Deploy Windows Hello for Business.

Answer: B

Explanation:

Add CA1 as a Certificate Authority to the Microsoft Entra ID tenant.

Question: 276 CertyIQ

You have accounts for the following cloud platforms:

•Azure
•Alibaba Cloud
•Amazon Web Services (AWS)
•Google Cloud Platform (GCP)

You configure an Azure subscription to use Microsoft Entra Permissions Management to manage the permissions in Azure only.

Which additional cloud platforms can be managed by using Permissions Management?

A.AWS only
B.Alibaba Cloud and AWS only
C.Alibaba Cloud and GCP only
D.AWS and GCP only
E.Alibaba Cloud, AWS, and GCP

Answer: D

Explanation:

Microsoft Entra Permissions Management is a cloud infrastructure entitlement management (CIEM) solution that provides comprehensive visibility into permissions assigned to all identities. For example, over-privileged workload and user identities, actions, and resources across multicloud infrastructures in Microsoft Azure, Amazon Web Services (AWS), and Google Cloud Platform (GCP).

Question: 277 CertyIQ

You have three Azure subscriptions that are linked to a single Microsoft Entra tenant.

You need to evaluate and remediate the risks associated with highly privileged accounts. The solution must minimize administrative effort.

What should you use?

A.Global Secure Access
B.Privileged Identity Management (PIM)
C.Microsoft Entra Permissions Management
D.Microsoft Entra Verified ID

Answer: C

Explanation:

Microsoft Entra Permissions Management.

Question: 278 CertyIQ

You have an Azure subscription named Sub1 that uses Microsoft Entra Permissions Management. Sub1 contains a user named User1. User1 is granted multiple permissions across Sub1.

You need to replace all the permissions granted to User1 with read-only permissions. The solution must minimize administrative effort.

What should you do on the Remediation tab in Permissions Management?

A.From the Role/Policy Template subtab, create a template.
B.From the My Requests subtab, create a new request.
C.From the Roles/Policies subtab, create a role.

D.From the Permissions subtab, use a quick action.

Answer: C

Explanation:

From the Roles/Policies subtab, create a role.

Reference:

https://learn.microsoft.com/en-us/training/permissions-management/explore-features-of-permissions-management/9-act-on-your-findings-with-remediation-tab

Question: 279 CertyIQ

You have an Azure subscription that contains a user named User1. The subscription is onboarded to Microsoft Entra Permissions Management.

You need to provide User1 with access to Permissions Management. The solution must meet the following requirements:

•Follow the principle of least privilege.
•Minimize administrative effort.

What should you do first?

A.From the Role/Policy Template subtab of Permissions Management, create a template.
B.From the Microsoft Entra admin center, create a security group.
C.From the My Requests subtab of Permissions Management, create a new request.
D.From the Microsoft Entra admin center, assign a role to User1.

Answer: B

Explanation:

From the Microsoft Entra admin center, create a security group.

Question: 280 CertyIQ

DRAG DROP
-

You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Description
User1	User	*Not applicable*
User2	User	*Not applicable*
Vault1	Azure Key Vault	Contains a secret named Secret1
Vault2	Azure Key Vault	Contains a secret named Secret2
Secret1	Secret	Stored in Vault1
Secret2	Secret	Stored in Vault2

The subscription uses Privileged Identity Management (PIM).

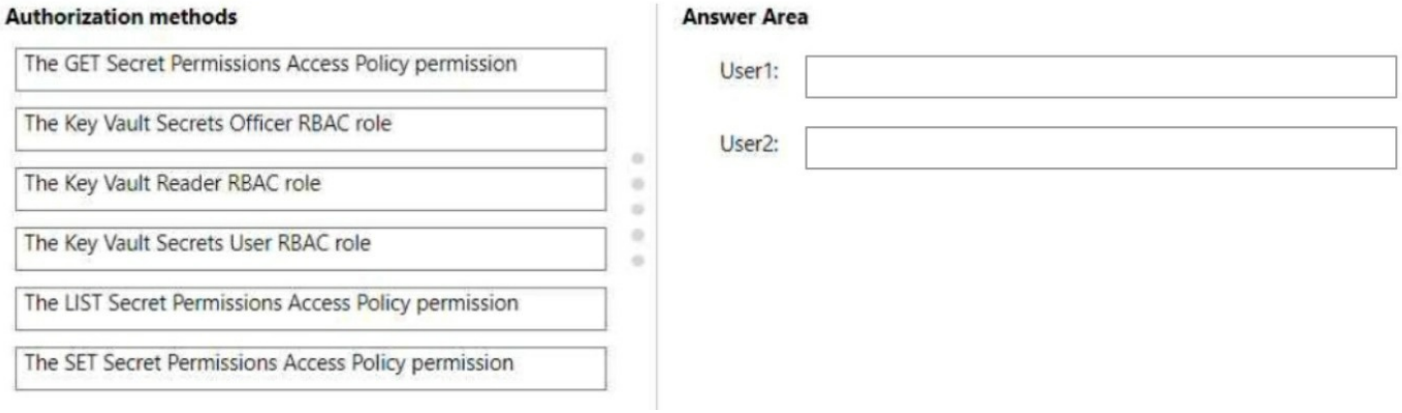
You need to configure the following access controls by using PIM:

•Ensure that User1 can read and update Secret1.
•Ensure that User2 can read the contents of the secrets stored in Vault2.

The solution must follow the principle of least privilege.

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

NOTE: Each correct selection is worth one point.



Answer:

Explanation:

The key vault Secrets officer RBAC role.

The key vault Secrets user RBAC role.

Question: 281 CertyIQ

HOTSPOT
-

You have two Azure subscriptions named Sub1 and Sub2 that are linked to a Microsoft Entra tenant. The tenant contains three groups named Group1, Group2, and Group3.

The subscriptions contain the resources shown in the following table.

Name	Type	Subscription
VM1	Virtual machine	Sub1
VM2	Virtual machine	Sub2
Automation1	Azure Automation account	Sub2

The tenant contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2, Group3
User3	Group3

You manage the subscriptions by using Microsoft Entra Permissions Management. Permissions Management is configured as shown in the following table.

Name	Roles	Authorization System Name	Requestor for Other Identities
Group1	Viewer	Sub1	*None*
Group2	Controller	Sub2	User1
Group3	Approver	All Current and Future	*None*

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 request access to VM2 by using Permissions Management.	○	○
User2 can create an access request to Automation1 on behalf of User1.	○	○
User3 can approve access requests for VM2.	○	○

Answer:

Answer Area

Statements	Yes	No
User1 can request access to VM2 by using Permissions Management.	○	○
User2 can create an access request to Automation1 on behalf of User1.	○	○
User3 can approve access requests for VM2.	○	○

Explanation:

No

Yes

Yes

Question: 282 CertyIQ

HOTSPOT
-

You have an Azure subscription that contains a user named User1.

You onboard Microsoft Entra Permissions Management.

You need to perform the following tasks:

•Identify all the accounts that are assigned the Global Administrator role permanently.
•Review the Permission Creep Index (PCI) of User1.

Which tab in Permissions Management should you use for each task? To answer, select the appropriate options in the answer area.

Answer Area

Identify all the accounts that are assigned the Global Administrator role permanently:

- Analytics
- Audit
- Azure AD Insights
- Dashboard
- Reports

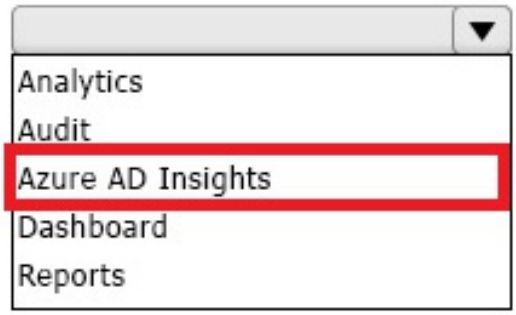
Review the PCI of User1:

- Analytics
- Audit
- Azure AD Insights
- Dashboard
- Reports

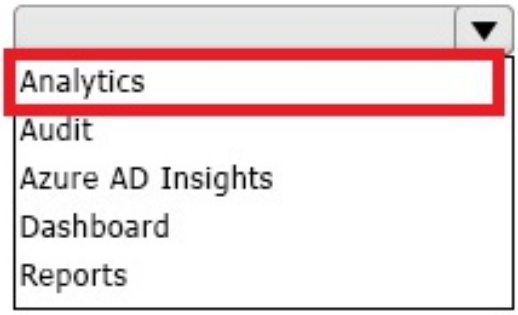
Answer:

Answer Area

Identify all the accounts that are assigned the Global Administrator role permanently:



Review the PCI of User1:



Explanation:

Azure AD Insights.

Analytics.

Question: 283 CertyIQ

You have an Azure subscription.

You need to use Microsoft Entra Permissions Management to automatically monitor permissions and create and implement right-size roles. The solution must follow the principle of least privilege.

Which role should you assign to the service principal of Permissions Management?

A.User Access Administrator
B.Contributor
C.Reader
D.Owner

Answer: B

Explanation:

Correct Answer B:To use Microsoft Entra Permissions Management to automatically monitor permissions and create and implement right-size roles while following the principle of least privilege, you should assign the Contributor role to the service principal12. This role provides the necessary permissions to manage resources without granting full administrative access.

Question: 284 CertyIQ

HOTSPOT
-

You have an Azure subscription named Sub1.

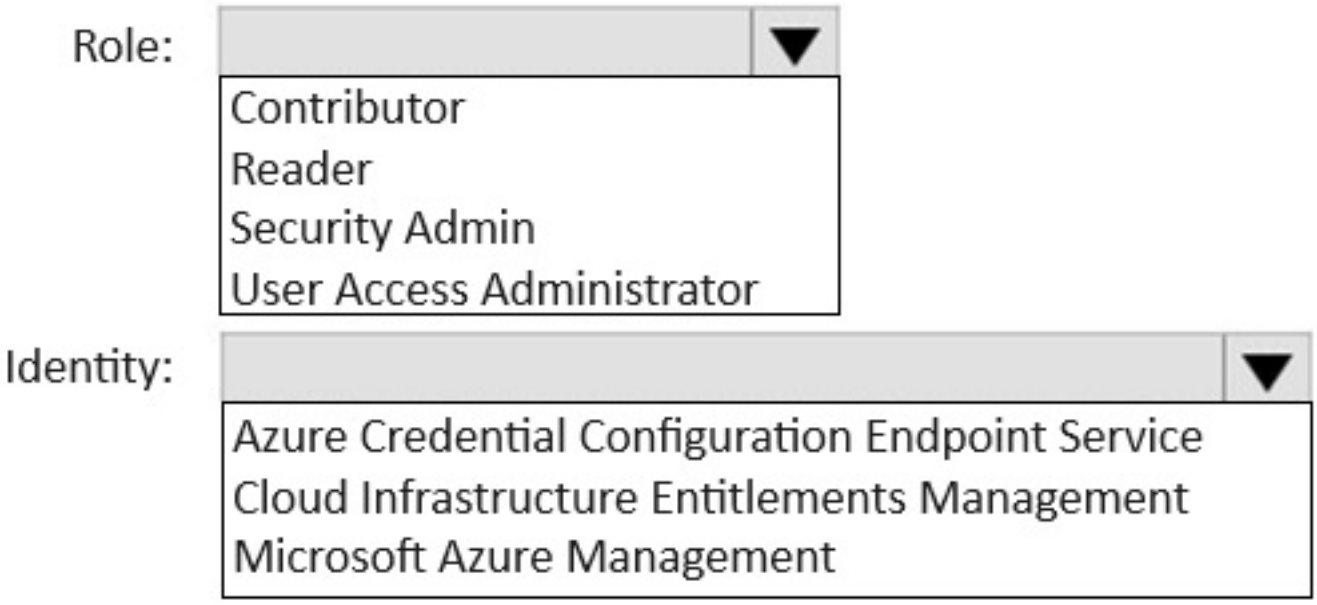
You plan to onboard Microsoft Entra Permissions Management.

You need to ensure that Permissions Management users can manage role assignments for Sub1. The solution must follow the principle of least privilege.

Which role should you assign and to which identity should you assign the role? To answer, select the appropriate options in the answer area.

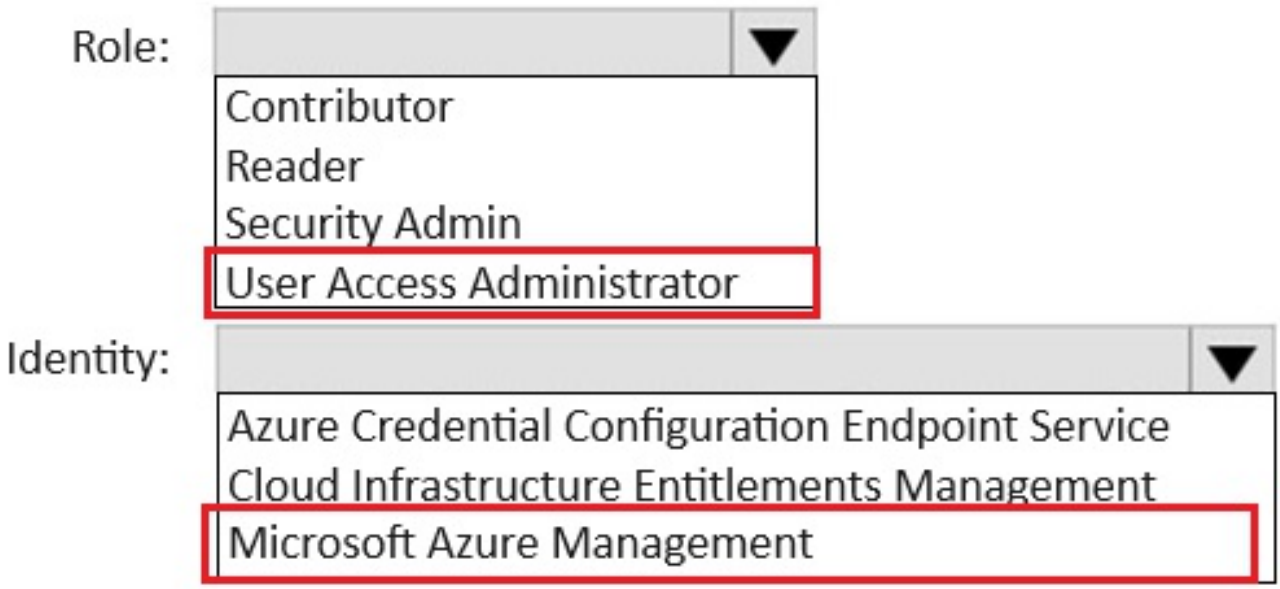
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area



Explanation:

Role: User Access Administrator .

Identity: Microsoft Azure Management.

Question: 285 CertyIQ

You have an Azure subscription, a Google Cloud Platform (GCP) account, and an Amazon Web Services (AWS) account.

You need to recommend a solution to assess the risks associated with privilege assignments across all the platforms. The solution must minimize administrative effort.

What should you include in the recommendation?

A.Microsoft Sentinel
B.Microsoft Entra ID Protection
C.Microsoft Defender for Cloud Apps
D.Microsoft Entra Permissions Management

Answer: D

Explanation:

D. Microsoft Entra Permissions ManagementMicrosoft Entra Permissions Management is the appropriate solution to assess the risks associated with privilege assignments across Azure, Google Cloud Platform (GCP), and Amazon Web Services (AWS) accounts. It provides centralized management and monitoring of permissions and access across multiple cloud platforms, helping identify and remediate risks associated with privilege assignments. By using Microsoft Entra Permissions Management, you can minimize administrative effort by having a single tool to manage permissions across different cloud environments.

Question: 286 CertyIQ

You have a Microsoft Entra tenant.

You need to configure continuous access evaluation for app sign-ins and assign the configuration to users that are assigned the Application Administrator role.

What should you configure?

A.a sign-in risk policy
B.an access review
C.a Conditional Access policy
D.the Admin consent settings

Answer: C

Explanation:

C. a Conditional Access policyTo configure continuous access evaluation for app sign-ins and assign the configuration to users that are assigned the Application Administrator role, you should configure a Conditional Access policy. Conditional Access policies in Microsoft Entra allow you to control access to apps and resources based on certain conditions such as user, location, device, and application state. By creating a Conditional Access policy, you can enable continuous access evaluation for app sign-ins and target the policy specifically to users assigned the Application Administrator role. This ensures that the configuration applies only to those users who have the appropriate role.

Question: 287 CertyIQ

Introductory Info Case Study -

Overview -
Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle.
Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.
Existing Environment. Existing Environment
The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named
Contoso_Resources. The Contoso_Resources OU contains all users and computers.
The contoso.com Active Directory domain contains the relevant users shown in the following table.

Name	Office	Department
Admin1	Montreal	Helpdesk
User1	Montreal	HR
User2	Montreal	HR
User3	Montreal	HR
Admin2	London	Helpdesk
User4	London	Finance
User5	London	Sales
User6	London	Sales
Admin3	Seattle	Helpdesk
User7	Seattle	Sales
User8	Seattle	Sales
User9	Seattle	Sales

Contoso also includes a marketing department that has users in each office.
Existing Environment. Microsoft 365/Azure Environment
Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:
Microsoft Office 365 Enterprise E5
Enterprise Mobility + Security E5
Windows 10 Enterprise E3
Project Plan 3
Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso_Resources OU is synced.
Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.
User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:
The users in the London office have the Microsoft 365 Phone System license unassigned.
The users in the Seattle office have the Yammer Enterprise license unassigned.
Security defaults are disabled for contoso.com.
Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.
Existing Environment. Problem Statements
Contoso identifies the following issues:
Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.
The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.
The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.
Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.
When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes -
Contoso plans to implement the following changes:
Implement self-service password reset (SSPR).
Analyze Azure audit activity logs by using Azure Monitor.
Simplify license allocation for new users added to the tenant.
Collaborate with the users at Fabrikam on a joint marketing campaign.
Configure the User administrator role to require justification and approval to activate.
Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.
For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.
Contoso plans to acquire a company named ADatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.
Requirements. Technical Requirements
Contoso identifies the following technical requirements:
All users must be synced from AD DS to the contoso.com Azure AD tenant.
App1 must have a redirect URI pointed to https://contoso.com/auth-response.

License allocation for new users must be assigned automatically based on the location of the user.
Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.
Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.
The helpdesk administrators must be able to manage licenses for only the users in their respective office.
Users must be forced to change their password if there is a probability that the users' identity was compromised.
Question You need to allocate licenses to the new users from ADatum. The solution must meet the technical requirements.
Which type of object should you create?

A. a Dynamic User security group
B. a distribution group
C. an OU
D. an administrative unit

Answer: A

Explanation:

You cannot assign licenses to an Administrative Unit, only a Group, see here https://learn.microsoft.com/en-us/answers/questions/955831/can-licenses-be-directly-assigned-to-an-administra.html

A must be the correct answer

Question: 288 CertyIQ

Introductory Info Case Study -

Overview -
Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle.
Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.
Existing Environment. Existing Environment
The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named
Contoso_Resources. The Contoso_Resources OU contains all users and computers.
The contoso.com Active Directory domain contains the relevant users shown in the following table.

Name	Office	Department
Admin1	Montreal	Helpdesk
User1	Montreal	HR
User2	Montreal	HR
User3	Montreal	HR
Admin2	London	Helpdesk
User4	London	Finance
User5	London	Sales
User6	London	Sales
Admin3	Seattle	Helpdesk
User7	Seattle	Sales
User8	Seattle	Sales
User9	Seattle	Sales

Contoso also includes a marketing department that has users in each office.
Existing Environment. Microsoft 365/Azure Environment
Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:
Microsoft Office 365 Enterprise E5

Enterprise Mobility + Security E5
Windows 10 Enterprise E3
Project Plan 3
Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso_Resources OU is synced.
Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.
User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:
The users in the London office have the Microsoft 365 Phone System license unassigned.
The users in the Seattle office have the Yammer Enterprise license unassigned.
Security defaults are disabled for contoso.com.
Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.
Existing Environment. Problem Statements
Contoso identifies the following issues:
Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.
The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.
The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.
Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.
When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes -
Contoso plans to implement the following changes:
Implement self-service password reset (SSPR).
Analyze Azure audit activity logs by using Azure Monitor.
Simplify license allocation for new users added to the tenant.
Collaborate with the users at Fabrikam on a joint marketing campaign.
Configure the User administrator role to require justification and approval to activate.
Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.
For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.
Contoso plans to acquire a company named ADatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.
Requirements. Technical Requirements
Contoso identifies the following technical requirements:
All users must be synced from AD DS to the contoso.com Azure AD tenant.
App1 must have a redirect URI pointed to https://contoso.com/auth-response.
License allocation for new users must be assigned automatically based on the location of the user.
Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.
Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.
The helpdesk administrators must be able to manage licenses for only the users in their respective office.
Users must be forced to change their password if there is a probability that the users' identity was compromised.
Question You need to sync the ADatum users. The solution must meet the technical requirements.
What should you do?

A. From the Microsoft Azure Active Directory Connect wizard, select Customize synchronization options.
B. From PowerShell, run Set-ADSyncScheduler.
C. From PowerShell, run Start-ADSyncSyncCycle.
D. From the Microsoft Azure Active Directory Connect wizard, select Change user sign-in.

Answer: A

Explanation:

You need to select Customize synchronization options to configure Azure AD Connect to sync the Adatum organizational unit (OU).

- Only Contoso_Resources OU is synced (if you run PS command it will sync only this OU)

- You need to also sync new OU Adatum in Contonso AD where new users were created

To do it you need to run AAD Connect , open "customize synchronization options"

and add Adatum OU.

All necessary details can be found here:

https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-installation-wizard#customize-synchronization-options

Question: 289 CertyIQ

Introductory Info Case Study -

Overview -
Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle.
Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.
Existing Environment. Existing Environment
The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named
Contoso_Resources. The Contoso_Resources OU contains all users and computers.
The contoso.com Active Directory domain contains the relevant users shown in the following table.

Name	Office	Department
Admin1	Montreal	Helpdesk
User1	Montreal	HR
User2	Montreal	HR
User3	Montreal	HR
Admin2	London	Helpdesk
User4	London	Finance
User5	London	Sales
User6	London	Sales
Admin3	Seattle	Helpdesk
User7	Seattle	Sales
User8	Seattle	Sales
User9	Seattle	Sales

Contoso also includes a marketing department that has users in each office.
Existing Environment. Microsoft 365/Azure Environment
Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:
Microsoft Office 365 Enterprise E5
Enterprise Mobility + Security E5
Windows 10 Enterprise E3
Project Plan 3
Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso_Resources OU is synced.
Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.
User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:
The users in the London office have the Microsoft 365 Phone System license unassigned.
The users in the Seattle office have the Yammer Enterprise license unassigned.
Security defaults are disabled for contoso.com.
Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.
Existing Environment. Problem Statements

Contoso identifies the following issues:
Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.
The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.
The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.
Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.
When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes -
Contoso plans to implement the following changes:
Implement self-service password reset (SSPR).
Analyze Azure audit activity logs by using Azure Monitor.
Simplify license allocation for new users added to the tenant.
Collaborate with the users at Fabrikam on a joint marketing campaign.
Configure the User administrator role to require justification and approval to activate.
Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.
For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.
Contoso plans to acquire a company named ADatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.
Requirements. Technical Requirements
Contoso identifies the following technical requirements:
All users must be synced from AD DS to the contoso.com Azure AD tenant.
App1 must have a redirect URI pointed to https://contoso.com/auth-response.
License allocation for new users must be assigned automatically based on the location of the user.
Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.
Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.
The helpdesk administrators must be able to manage licenses for only the users in their respective office.
Users must be forced to change their password if there is a probability that the users' identity was compromised.
Question HOTSPOT -
You need to meet the technical requirements for license management by the helpdesk administrators.
What should you create first, and which tool should you use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

Object to create for each branch office:

- An administrative unit
- A custom role
- A Dynamic User security group
- An OU

Tool to use:

- Azure Active Directory admin center
- Active Directory Administrative Center
- Active Directory module for Windows PowerShell
- Microsoft 365 admin center

Answer:

Answer Area

Object to create for each branch office:

- An administrative unit
- A custom role
- A Dynamic User security group
- An OU

Tool to use:

- Azure Active Directory admin center
- Active Directory Administrative Center
- Active Directory module for Windows PowerShell
- Microsoft 365 admin center

Explanation:

Q1: Administrative Units. This would limit the scope of admins as required.

Q2: AAD Admin Center (not the on-prem Active Directory Administrative Center)

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/roles/administrative-units
https://docs.microsoft.com/en-us/azure/active-directory/roles/admin-units-manage

Question: 290 CertyIQ

Introductory Info Case Study -

Overview -
Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle.
Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.
Existing Environment. Existing Environment
The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named
Contoso_Resources. The Contoso_Resources OU contains all users and computers.
The contoso.com Active Directory domain contains the relevant users shown in the following table.

Name	Office	Department
Admin1	Montreal	Helpdesk
User1	Montreal	HR
User2	Montreal	HR
User3	Montreal	HR
Admin2	London	Helpdesk
User4	London	Finance
User5	London	Sales
User6	London	Sales
Admin3	Seattle	Helpdesk
User7	Seattle	Sales
User8	Seattle	Sales
User9	Seattle	Sales

Contoso also includes a marketing department that has users in each office.
Existing Environment. Microsoft 365/Azure Environment
Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:
Microsoft Office 365 Enterprise E5
Enterprise Mobility + Security E5
Windows 10 Enterprise E3
Project Plan 3
Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso_Resources OU is synced.
Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.
User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:
The users in the London office have the Microsoft 365 Phone System license unassigned.
The users in the Seattle office have the Yammer Enterprise license unassigned.
Security defaults are disabled for contoso.com.
Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.
Existing Environment. Problem Statements
Contoso identifies the following issues:
Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.
The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.
The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.
Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.
When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes -
Contoso plans to implement the following changes:
Implement self-service password reset (SSPR).
Analyze Azure audit activity logs by using Azure Monitor.
Simplify license allocation for new users added to the tenant.
Collaborate with the users at Fabrikam on a joint marketing campaign.
Configure the User administrator role to require justification and approval to activate.
Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.
For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.
Contoso plans to acquire a company named ADatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.
Requirements. Technical Requirements
Contoso identifies the following technical requirements:
All users must be synced from AD DS to the contoso.com Azure AD tenant.
App1 must have a redirect URI pointed to https://contoso.com/auth-response.

License allocation for new users must be assigned automatically based on the location of the user.
Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.
Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.
The helpdesk administrators must be able to manage licenses for only the users in their respective office.
Users must be forced to change their password if there is a probability that the users' identity was compromised.
Question You need to resolve the issue of the sales department users.
What should you configure for the Azure AD tenant?

A. the Device settings
B. the Access reviews settings
C. the User settings
D. Security defaults

Answer: C

Explanation:

Scenario: There are Sales department users in London and in Seattle.

* The users in the London office have the Microsoft 365 Phone System license unassigned.

* The users in the Seattle office have the Yammer Enterprise license unassigned.

Use the Active users page to unassign licenses.

When you use the Active users page to unassign licenses, you unassign product licenses from users.

Unassign licenses from one user.

1. In the admin center, go to the Users > Active users page.

2. Select the row of the user that you want to unassign a license for.

3. In the right pane, select Licenses and Apps.

4. Expand the Licenses section, clear the boxes for the licenses that you want to unassign, then select Save changes.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/admin/manage/remove-licenses-from-users

Question: 291 CertyIQ

Introductory Info Case Study -

Overview -
Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.
Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.
Existing Environment. Identity Environment
The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD
Connect uses pass-through authentication and has password hash synchronization disabled.
Litware.com contains a user named User1 who oversees all application development.
Litware implements Azure AD Application Proxy.
Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.
Existing Environment. Cloud Environment
All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in

Microsoft Cloud App Security are enabled.
Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active
Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.
Existing Environment. On-premises Environment
The on-premises network contains the servers shown in the following table.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller for litware.com
SERVER1	Windows Server 2019	Boston	Member server in litware.com that runs the Azure AD Application Proxy connector
SERVER2	Windows Server 2019	Boston	Member server that uses Azure AD Connect

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.
Requirements. Delegation Requirements
Litware identifies the following delegation requirements:
Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).
Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.
Use custom programs for Identity Governance.
Ensure that User1 can create enterprise applications in Azure AD.
Use the principle of least privilege.
Requirements. Licensing Requirements
Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest.
Litware wants to manage the assignment of Azure
AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to a
Microsoft 365 group that has the appropriate licenses assigned.
Requirements. Management Requirements
Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.
Requirements. Authentication Requirements
Litware identifies the following authentication requirements:
Implement multi-factor authentication (MFA) for all Litware users by using conditional access policies.
Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.
Implement a banned password list for the litware.com forest.
Enforce MFA when accessing on-premises applications.
Automatically detect and remediate externally leaked credentials.
Requirements. Access Requirements
Litware identifies the following access requirements:
Control all access to all Azure resources and Azure AD applications by using conditional access policies.
Implement a conditional access policy that has session controls for Microsoft SharePoint Online.
Control privileged access to applications by using access reviews in Azure AD.
Requirements. Monitoring Requirements
Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged attacks that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity. Question HOTSPOT -
You need to configure the assignment of Azure AD licenses to the Litware users. The solution must meet the licensing requirements.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

Azure AD Connect settings to modify:

- Directory Extensions
- Domain Filtering
- Optional Features

Assign Azure AD licenses to:

- An Azure Active Directory group that has only nested groups
- An Azure Active Directory group that has the Assigned membership type
- An Azure Active Directory group that has the Dynamic User membership type

Answer:

Answer Area

Azure AD Connect settings to modify:

- Directory Extensions
- Domain Filtering
- Optional Features

Assign Azure AD licenses to:

- An Azure Active Directory group that has only nested groups
- An Azure Active Directory group that has the Assigned membership type
- An Azure Active Directory group that has the Dynamic User membership type

Explanation:

Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest. Litware wants to manage the assignment of Azure
AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to a
Microsoft 365 group that has the appropriate licenses assigned.

Question: 292

CertyIQ

Introductory Info Case Study -

Overview -
Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.
Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.
Existing Environment. Identity Environment
The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD
Connect uses pass-through authentication and has password hash synchronization disabled.
Litware.com contains a user named User1 who oversees all application development.
Litware implements Azure AD Application Proxy.
Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.
Existing Environment. Cloud Environment
All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.
Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active
Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.
Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller for litware.com
SERVER1	Windows Server 2019	Boston	Member server in litware.com that runs the Azure AD Application Proxy connector
SERVER2	Windows Server 2019	Boston	Member server that uses Azure AD Connect

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.
Requirements. Delegation Requirements
Litware identifies the following delegation requirements:
Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).
Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.
Use custom programs for Identity Governance.
Ensure that User1 can create enterprise applications in Azure AD.
Use the principle of least privilege.
Requirements. Licensing Requirements
Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest.
Litware wants to manage the assignment of Azure
AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to a
Microsoft 365 group that has the appropriate licenses assigned.
Requirements. Management Requirements
Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.
Requirements. Authentication Requirements
Litware identifies the following authentication requirements:
Implement multi-factor authentication (MFA) for all Litware users by using conditional access policies.
Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.
Implement a banned password list for the litware.com forest.
Enforce MFA when accessing on-premises applications.
Automatically detect and remediate externally leaked credentials.
Requirements. Access Requirements
Litware identifies the following access requirements:
Control all access to all Azure resources and Azure AD applications by using conditional access policies.
Implement a conditional access policy that has session controls for Microsoft SharePoint Online.
Control privileged access to applications by using access reviews in Azure AD.
Requirements. Monitoring Requirements
Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged attacks that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity. Question You need to meet the authentication requirements for leaked credentials.
What should you do?

A. Enable password hash synchronization in Azure AD Connect.
B. Configure Azure AD Password Protection.
C. Configure an authentication method policy in Azure AD.
D. Enable federation with PingFederate in Azure AD Connect.

Answer: A

Explanation:

Password hash synchronization

"Risk detections like leaked credentials require the presence of password hashes for detection to occur. For

more information about password hash synchronization, see the article, Implement password hash synchronization with Azure AD Connect sync."

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks#password-hash-synchronization

Reference:

https://docs.microsoft.com/en-us/azure/security/fundamentals/steps-secure-identity

Question: 293 CertyIQ

Introductory Info Case Study -

Overview -
Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.
Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.
Existing Environment. Identity Environment
The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD
Connect uses pass-through authentication and has password hash synchronization disabled.
Litware.com contains a user named User1 who oversees all application development.
Litware implements Azure AD Application Proxy.
Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.
Existing Environment. Cloud Environment
All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.
Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active
Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.
Existing Environment. On-premises Environment
The on-premises network contains the servers shown in the following table.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller for litware.com
SERVER1	Windows Server 2019	Boston	Member server in litware.com that runs the Azure AD Application Proxy connector
SERVER2	Windows Server 2019	Boston	Member server that uses Azure AD Connect

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.
Requirements. Delegation Requirements
Litware identifies the following delegation requirements:
Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).
Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.
Use custom programs for Identity Governance.
Ensure that User1 can create enterprise applications in Azure AD.
Use the principle of least privilege.
Requirements. Licensing Requirements
Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest.
Litware wants to manage the assignment of Azure
AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for

LWLicenses must be added automatically to a
Microsoft 365 group that has the appropriate licenses assigned.
Requirements. Management Requirements
Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.
Requirements. Authentication Requirements
Litware identifies the following authentication requirements:
Implement multi-factor authentication (MFA) for all Litware users by using conditional access policies.
Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.

- Implement a banned password list for the litware.com forest.
- Enforce MFA when accessing on-premises applications.
- Automatically detect and remediate externally leaked credentials.

Requirements. Access Requirements
Litware identifies the following access requirements:
Control all access to all Azure resources and Azure AD applications by using conditional access policies.
Implement a conditional access policy that has session controls for Microsoft SharePoint Online.
Control privileged access to applications by using access reviews in Azure AD.
Requirements. Monitoring Requirements
Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged attacks that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity. Question HOTSPOT -
You need to identify which roles to use for managing role assignments. The solution must meet the delegation requirements.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

To manage Azure AD built-in role assignments, use:

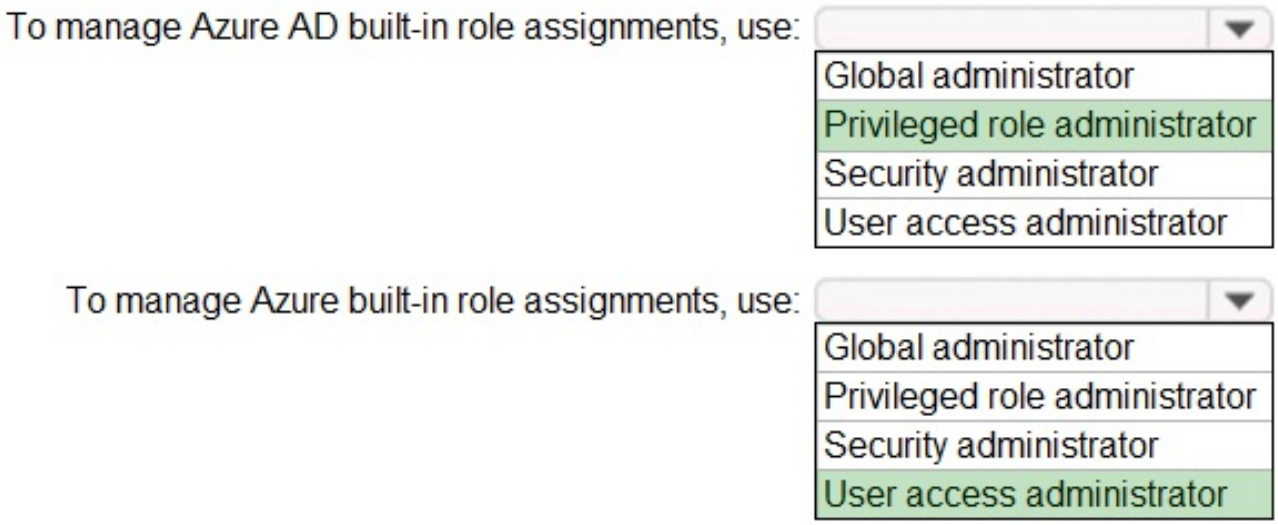
- Global administrator
- Privileged role administrator
- Security administrator
- User access administrator

To manage Azure built-in role assignments, use:

- Global administrator
- Privileged role administrator
- Security administrator
- User access administrator

Answer:

Answer Area



Explanation:

For Azure AD roles in Privileged Identity Management, only a user who is in the Privileged Role Administrator or Global Administrator role can manage assignments for other administrators. Global Administrators, Security Administrators, Global Readers, and Security Readers can also view assignments to Azure AD roles in Privileged Identity Management.

For Azure resource roles in Privileged Identity Management, only a subscription administrator, a resource Owner, or a resource User Access administrator can manage assignments for other administrators. Users who are Privileged Role Administrators, Security Administrators, or Security Readers do not by default have access to view assignments to Azure resource roles in Privileged Identity Management.

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

Reference:

https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

Question: 294 CertyIQ

Introductory Info Case Study -

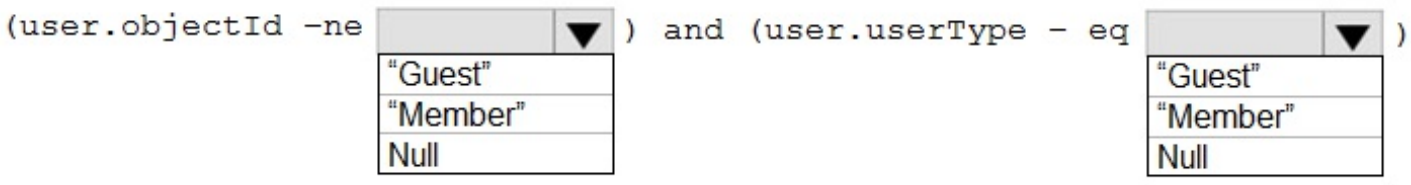
Overview -
Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.
Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.
Existing Environment. Identity Environment
The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD
Connect uses pass-through authentication and has password hash synchronization disabled.
Litware.com contains a user named User1 who oversees all application development.
Litware implements Azure AD Application Proxy.
Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.
Existing Environment. Cloud Environment
All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.
Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an

Azure Sentinel instance that uses the Azure Active
Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.
Existing Environment. On-premises Environment
The on-premises network contains the servers shown in the following table.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller for litware.com
SERVER1	Windows Server 2019	Boston	Member server in litware.com that runs the Azure AD Application Proxy connector
SERVER2	Windows Server 2019	Boston	Member server that uses Azure AD Connect

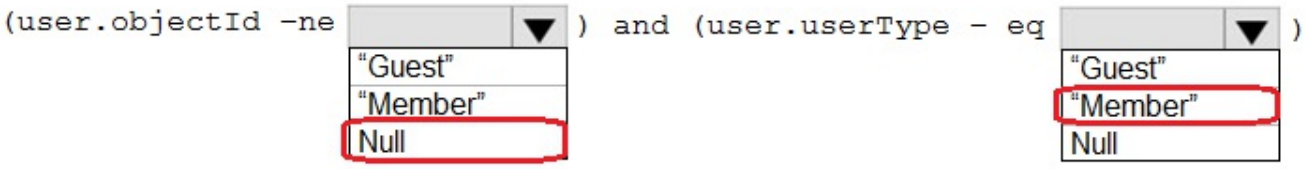
Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.
Requirements. Delegation Requirements
Litware identifies the following delegation requirements:
Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).
Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.
Use custom programs for Identity Governance.
Ensure that User1 can create enterprise applications in Azure AD.
Use the principle of least privilege.
Requirements. Licensing Requirements
Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest.
Litware wants to manage the assignment of Azure
AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to a
Microsoft 365 group that has the appropriate licenses assigned.
Requirements. Management Requirements
Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.
Requirements. Authentication Requirements
Litware identifies the following authentication requirements:
Implement multi-factor authentication (MFA) for all Litware users by using conditional access policies.
Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.
- Implement a banned password list for the litware.com forest.
Enforce MFA when accessing on-premises applications.
Automatically detect and remediate externally leaked credentials.
Requirements. Access Requirements
Litware identifies the following access requirements:
Control all access to all Azure resources and Azure AD applications by using conditional access policies.
Implement a conditional access policy that has session controls for Microsoft SharePoint Online.
Control privileged access to applications by using access reviews in Azure AD.
Requirements. Monitoring Requirements
Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged attacks that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity. Question HOTSPOT -
You need to create the LWGroup1 group to meet the management requirements.
How should you complete the dynamic membership rule? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area



Answer:

Answer Area



Explanation:

It's NULL and MEMBER

This link explains it 100% - https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership#:~:text=If%20you%20want%20your,user.userType%20%2Deq%20%22Member%22)

REQ: Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.

Creating a group of members only

If you want your group to exclude guest users and include only members of your tenant, create a dynamic group as described above, but in the Rule syntax box, enter the following expression:

(user.objectId -ne **null**) and (user.userType -eq "**Member**")

https://docs.microsoft.com/en-us/azure/active-directory/external-identities/use-dynamic-groups#creating-a-group-of-members-only

Question: 295 CertyIQ

Introductory Info Case Study -

Overview -
Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle.
Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.
Existing Environment. Existing Environment
The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named
Contoso_Resources. The Contoso_Resources OU contains all users and computers.
The contoso.com Active Directory domain contains the relevant users shown in the following table.

Name	Office	Department
Admin1	Montreal	Helpdesk
User1	Montreal	HR
User2	Montreal	HR
User3	Montreal	HR
Admin2	London	Helpdesk
User4	London	Finance
User5	London	Sales
User6	London	Sales
Admin3	Seattle	Helpdesk
User7	Seattle	Sales
User8	Seattle	Sales
User9	Seattle	Sales

Contoso also includes a marketing department that has users in each office.
Existing Environment. Microsoft 365/Azure Environment
Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:
Microsoft Office 365 Enterprise E5
Enterprise Mobility + Security E5
Windows 10 Enterprise E3
Project Plan 3
Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso_Resources OU is synced.
Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.
User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:
The users in the London office have the Microsoft 365 Phone System license unassigned.
The users in the Seattle office have the Yammer Enterprise license unassigned.
Security defaults are disabled for contoso.com.
Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.
Existing Environment. Problem Statements
Contoso identifies the following issues:
Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.
The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.
The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.
Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.
When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes -
Contoso plans to implement the following changes:
Implement self-service password reset (SSPR).
Analyze Azure audit activity logs by using Azure Monitor.
Simplify license allocation for new users added to the tenant.
Collaborate with the users at Fabrikam on a joint marketing campaign.
Configure the User administrator role to require justification and approval to activate.
Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.
For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.
Contoso plans to acquire a company named ADatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.
Requirements. Technical Requirements
Contoso identifies the following technical requirements:
All users must be synced from AD DS to the contoso.com Azure AD tenant.
App1 must have a redirect URI pointed to https://contoso.com/auth-response.

License allocation for new users must be assigned automatically based on the location of the user.
Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.
Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.
The helpdesk administrators must be able to manage licenses for only the users in their respective office.
Users must be forced to change their password if there is a probability that the users' identity was compromised.
Question HOTSPOT -
You need to meet the technical requirements for the probability that user identities were compromised.
What should the users do first, and what should you configure? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

The users must first:

- Provide consent for any app to access the data of Contoso.
- Register for multi-factor authentication (MFA).
- Register for self-service password reset (SSPR).

You must configure:

- A sign-in risk policy
- A user risk policy
- An Azure AD Password Protection policy

Answer:

Answer Area

The users must first:

- Provide consent for any app to access the data of Contoso.
- Register for multi-factor authentication (MFA).
- Register for self-service password reset (SSPR). ✓

You must configure:

- A sign-in risk policy
- A user risk policy ✓
- An Azure AD Password Protection policy

Explanation:

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

Question: 296

Introductory Info Case Study -

Overview -
Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.
Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.
Existing Environment. Identity Environment
The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD
Connect uses pass-through authentication and has password hash synchronization disabled.
Litware.com contains a user named User1 who oversees all application development.
Litware implements Azure AD Application Proxy.
Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.
Existing Environment. Cloud Environment
All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.
Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active
Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.
Existing Environment. On-premises Environment
The on-premises network contains the servers shown in the following table.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller for litware.com
SERVER1	Windows Server 2019	Boston	Member server in litware.com that runs the Azure AD Application Proxy connector
SERVER2	Windows Server 2019	Boston	Member server that uses Azure AD Connect

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.
Requirements. Delegation Requirements
Litware identifies the following delegation requirements:
Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).
Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.
Use custom programs for Identity Governance.
Ensure that User1 can create enterprise applications in Azure AD.
Use the principle of least privilege.
Requirements. Licensing Requirements
Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest.
Litware wants to manage the assignment of Azure
AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to a
Microsoft 365 group that has the appropriate licenses assigned.
Requirements. Management Requirements
Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.
Requirements. Authentication Requirements
Litware identifies the following authentication requirements:
Implement multi-factor authentication (MFA) for all Litware users by using conditional access policies.
Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.
- Implement a banned password list for the litware.com forest.
- Enforce MFA when accessing on-premises applications.
- Automatically detect and remediate externally leaked credentials.

Requirements. Access Requirements
Litware identifies the following access requirements:
Control all access to all Azure resources and Azure AD applications by using conditional access policies.

Implement a conditional access policy that has session controls for Microsoft SharePoint Online.
Control privileged access to applications by using access reviews in Azure AD.
Requirements. Monitoring Requirements
Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged attacks that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity. Question You need to configure the MFA settings for users who connect from the Boston office. The solution must meet the authentication requirements and the access requirements.
What should you include in the configuration?

A. named locations that have a private IP address range
B. named locations that have a public IP address range
C. trusted IPs that have a public IP address range
D. trusted IPs that have a private IP address range

Answer: B

Explanation:

Named Locations are part of Conditional Access Policies whereas "Trusted IPs" are in the legacy MFA settings, which would not be preferred.

The IP address will appear to be coming into Azure from the NAT'd public address not the internal network private address.

So I'd say: B. named locations that have a public IP address range

Question: 297 CertyIQ

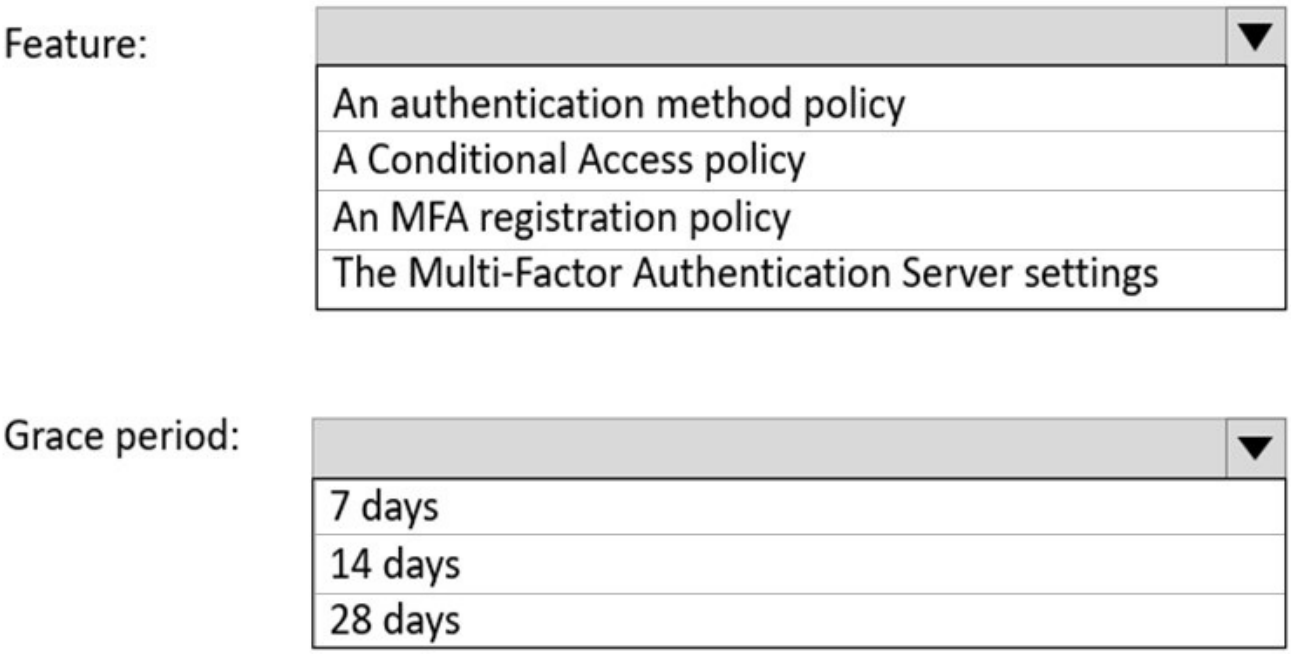
Introductory Info Case Study -

Overview -
Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.
Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.
Existing Environment. Identity Environment
The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD
Connect uses pass-through authentication and has password hash synchronization disabled.
Litware.com contains a user named User1 who oversees all application development.
Litware implements Azure AD Application Proxy.
Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.
Existing Environment. Cloud Environment
All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.
Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active
Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.
Existing Environment. On-premises Environment
The on-premises network contains the servers shown in the following table.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller for litware.com
SERVER1	Windows Server 2019	Boston	Member server in litware.com that runs the Azure AD Application Proxy connector
SERVER2	Windows Server 2019	Boston	Member server that uses Azure AD Connect

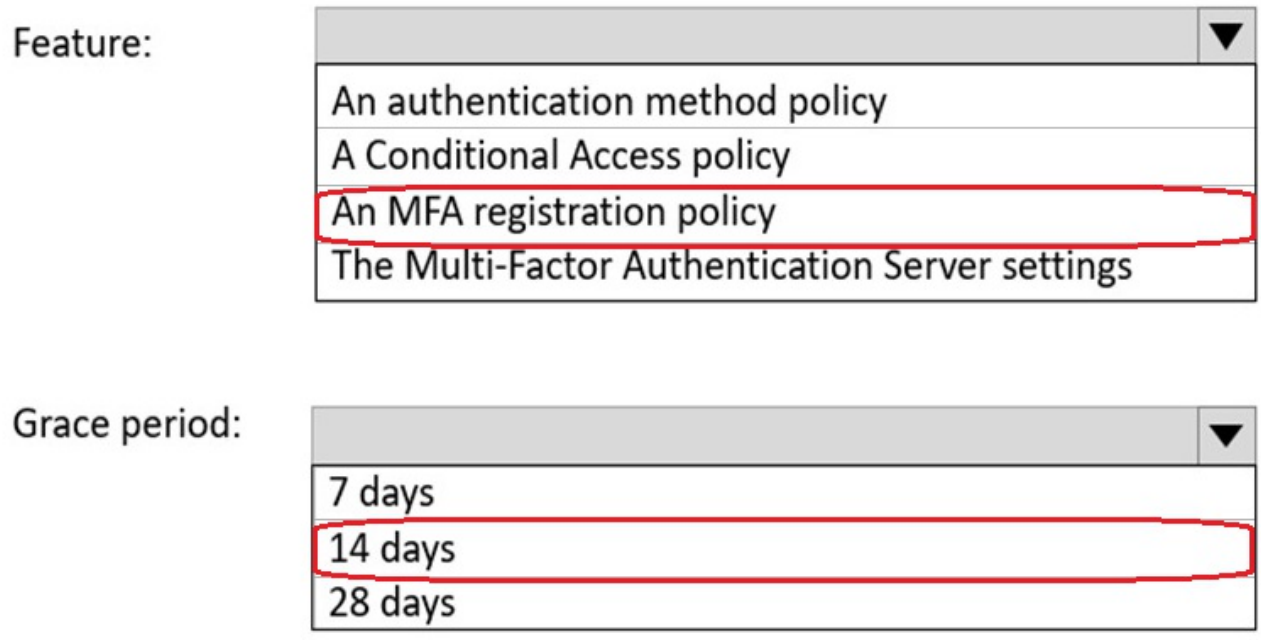
Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.
Requirements. Delegation Requirements
Litware identifies the following delegation requirements:
Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).
Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.
Use custom programs for Identity Governance.
Ensure that User1 can create enterprise applications in Azure AD.
Use the principle of least privilege.
Requirements. Licensing Requirements
Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest.
Litware wants to manage the assignment of Azure
AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to a
Microsoft 365 group that has the appropriate licenses assigned.
Requirements. Management Requirements
Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.
Requirements. Authentication Requirements
Litware identifies the following authentication requirements:
Implement multi-factor authentication (MFA) for all Litware users by using conditional access policies.
Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.
Implement a banned password list for the litware.com forest.
Enforce MFA when accessing on-premises applications.
Automatically detect and remediate externally leaked credentials.
Requirements. Access Requirements
Litware identifies the following access requirements:
Control all access to all Azure resources and Azure AD applications by using conditional access policies.
Implement a conditional access policy that has session controls for Microsoft SharePoint Online.
Control privileged access to applications by using access reviews in Azure AD.
Requirements. Monitoring Requirements
Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged attacks that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity. Question HOTSPOT -
You need to support the planned changes and meet the technical requirements for MFA.
Which feature should you use, and how long before the users must complete the registration? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area



Answer:

Answer Area



Explanation:

Box 1: MFA registration policy

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-mfa-policy#policy-configuration

Box 2: 14 days -

Multi-factor authentication (MFA): multi-factor authentication is a type of authentication that requires the use of two or more verification factors to gain access to a system. Azure MFA offers a 14 day grace period after being initiated.

Reference:

https://www.syskit.com/blog/using-azure-conditional-access-when-security-defaults-isnt-enough/

Question: 298 CertyIQ

Introductory Info Case Study -

Overview -
Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle.
Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.
Existing Environment. Existing Environment
The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named
Contoso_Resources. The Contoso_Resources OU contains all users and computers.
The contoso.com Active Directory domain contains the relevant users shown in the following table.

Name	Office	Department
Admin1	Montreal	Helpdesk
User1	Montreal	HR
User2	Montreal	HR
User3	Montreal	HR
Admin2	London	Helpdesk
User4	London	Finance
User5	London	Sales
User6	London	Sales
Admin3	Seattle	Helpdesk
User7	Seattle	Sales
User8	Seattle	Sales
User9	Seattle	Sales

Contoso also includes a marketing department that has users in each office.
Existing Environment. Microsoft 365/Azure Environment
Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:
Microsoft Office 365 Enterprise E5
Enterprise Mobility + Security E5
Windows 10 Enterprise E3
Project Plan 3
Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso_Resources OU is synced.
Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.
User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:
The users in the London office have the Microsoft 365 Phone System license unassigned.
The users in the Seattle office have the Yammer Enterprise license unassigned.
Security defaults are disabled for contoso.com.
Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.
Existing Environment. Problem Statements
Contoso identifies the following issues:

Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.
The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.
The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.
Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.
When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes -
Contoso plans to implement the following changes:
Implement self-service password reset (SSPR).
Analyze Azure audit activity logs by using Azure Monitor.
Simplify license allocation for new users added to the tenant.
Collaborate with the users at Fabrikam on a joint marketing campaign.
Configure the User administrator role to require justification and approval to activate.
Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.
For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.
Contoso plans to acquire a company named ADatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.
Requirements. Technical Requirements
Contoso identifies the following technical requirements:
All users must be synced from AD DS to the contoso.com Azure AD tenant.
App1 must have a redirect URI pointed to https://contoso.com/auth-response.
License allocation for new users must be assigned automatically based on the location of the user.
Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.
Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.
The helpdesk administrators must be able to manage licenses for only the users in their respective office.
Users must be forced to change their password if there is a probability that the users' identity was compromised.
Question You need to meet the planned changes and technical requirements for App1.
What should you implement?

A. a policy set in Microsoft Endpoint Manager
B. an app configuration policy in Microsoft Endpoint Manager
C. an app registration in Azure AD
D. Azure AD Application Proxy

Answer: C

Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app

Question: 299 CertyIQ

Introductory Info Case Study -

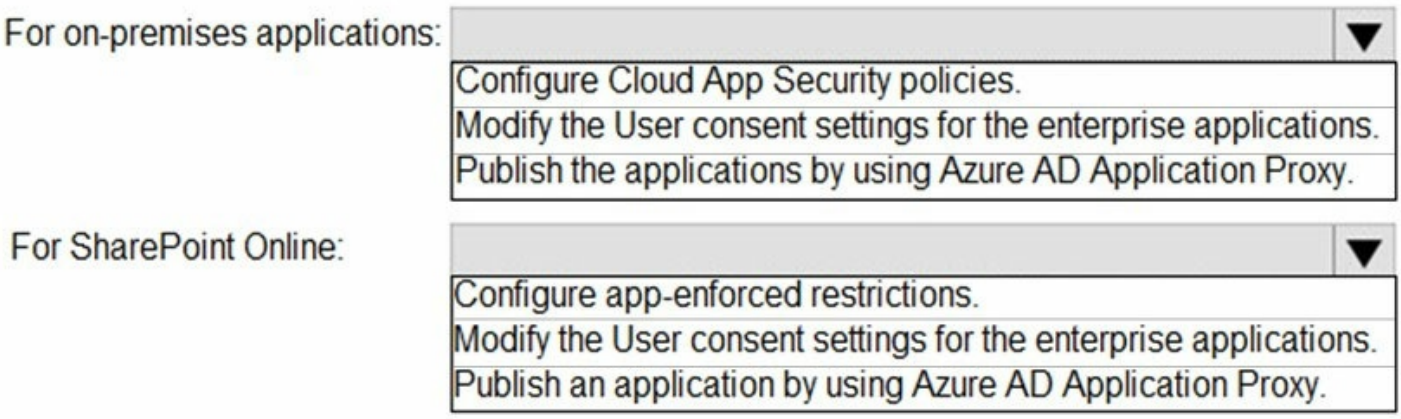
Overview -
Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.
Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.
Existing Environment. Identity Environment
The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD
Connect uses pass-through authentication and has password hash synchronization disabled.
Litware.com contains a user named User1 who oversees all application development.
Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.
Existing Environment. Cloud Environment
All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.
Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active
Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.
Existing Environment. On-premises Environment
The on-premises network contains the servers shown in the following table.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller for litware.com
SERVER1	Windows Server 2019	Boston	Member server in litware.com that runs the Azure AD Application Proxy connector
SERVER2	Windows Server 2019	Boston	Member server that uses Azure AD Connect

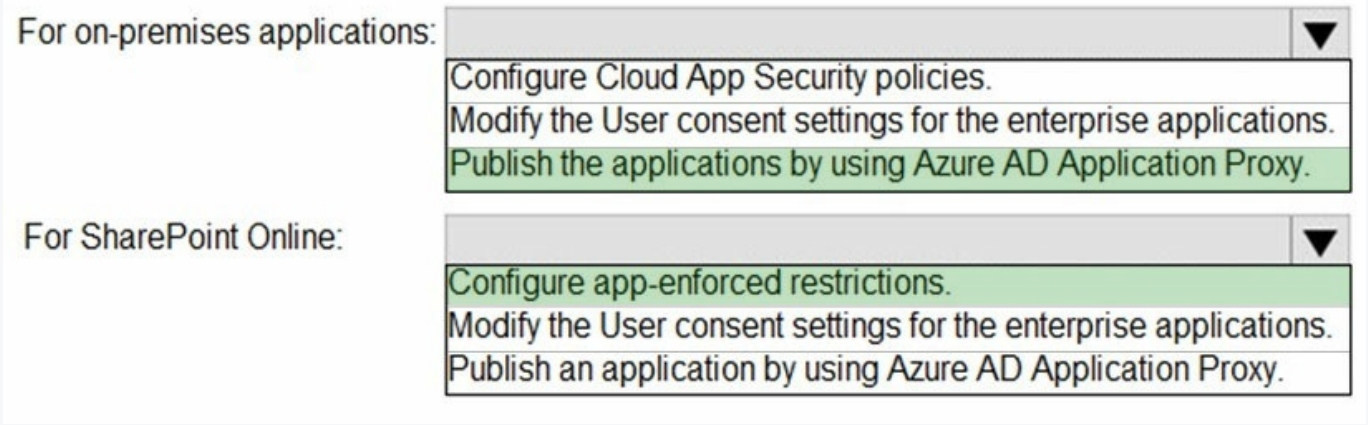
Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.
Requirements. Delegation Requirements
Litware identifies the following delegation requirements:
Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).
Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.
Use custom programs for Identity Governance.
Ensure that User1 can create enterprise applications in Azure AD.
Use the principle of least privilege.
Requirements. Licensing Requirements
Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest.
Litware wants to manage the assignment of Azure
AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to a
Microsoft 365 group that has the appropriate licenses assigned.
Requirements. Management Requirements
Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.
Requirements. Authentication Requirements
Litware identifies the following authentication requirements:
Implement multi-factor authentication (MFA) for all Litware users by using conditional access policies.
Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.
- Implement a banned password list for the litware.com forest.
Enforce MFA when accessing on-premises applications.
Automatically detect and remediate externally leaked credentials.
Requirements. Access Requirements
Litware identifies the following access requirements:
Control all access to all Azure resources and Azure AD applications by using conditional access policies.
Implement a conditional access policy that has session controls for Microsoft SharePoint Online.
Control privileged access to applications by using access reviews in Azure AD.
Requirements. Monitoring Requirements
Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged attacks that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity. Question HOTSPOT -
You need to implement on-premises application and SharePoint Online restrictions to meet the authentication requirements and the access requirements.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area



Answer:

Answer Area



Explanation:

The requirement for on-premise applications is "Enforce MFA when accessing ...", as we have already

* Implement MFA for all Litware users (via Azure AD)

* Litware implements Azure AD Appliication Proxy

we just need to "Publish the applications by using Azure AD Application Proxy" - this will force users to use their Azure AD account (and MFA) to access the on-premise applications.

Reference:

https://docs.microsoft.com/en-us/sharepoint/app-enforced-restrictions https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session

Question: 300 CertyIQ

Introductory Info Case Study -

Overview -
Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.

Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.
Existing Environment. Identity Environment
The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD
Connect uses pass-through authentication and has password hash synchronization disabled.
Litware.com contains a user named User1 who oversees all application development.
Litware implements Azure AD Application Proxy.
Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.
Existing Environment. Cloud Environment
All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.
Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active
Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.
Existing Environment. On-premises Environment
The on-premises network contains the servers shown in the following table.

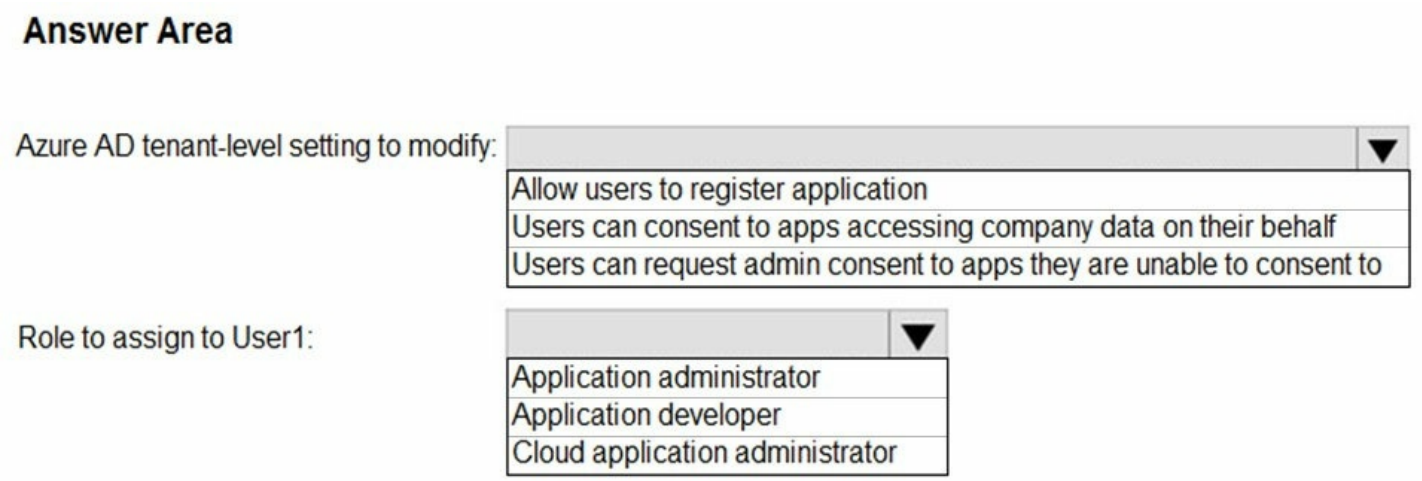
Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller for litware.com
SERVER1	Windows Server 2019	Boston	Member server in litware.com that runs the Azure AD Application Proxy connector
SERVER2	Windows Server 2019	Boston	Member server that uses Azure AD Connect

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.
Requirements. Delegation Requirements
Litware identifies the following delegation requirements:
Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).
Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.
Use custom programs for Identity Governance.
Ensure that User1 can create enterprise applications in Azure AD.
Use the principle of least privilege.
Requirements. Licensing Requirements
Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest.
Litware wants to manage the assignment of Azure
AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to a
Microsoft 365 group that has the appropriate licenses assigned.
Requirements. Management Requirements
Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.
Requirements. Authentication Requirements
Litware identifies the following authentication requirements:
Implement multi-factor authentication (MFA) for all Litware users by using conditional access policies.
Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.

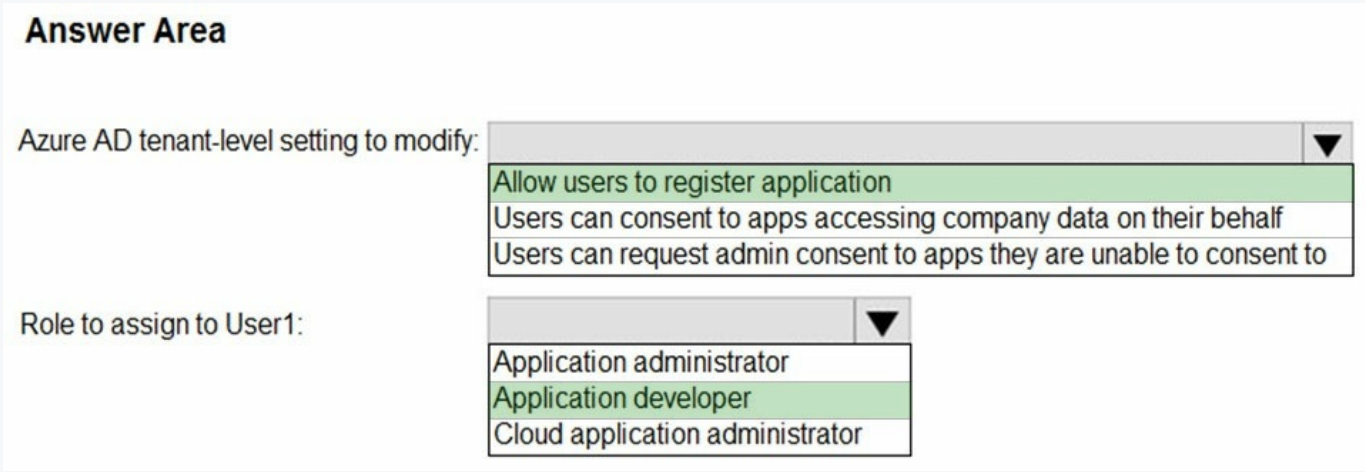
- Implement a banned password list for the litware.com forest.
- Enforce MFA when accessing on-premises applications.
- Automatically detect and remediate externally leaked credentials.

Requirements. Access Requirements
Litware identifies the following access requirements:
Control all access to all Azure resources and Azure AD applications by using conditional access policies.
Implement a conditional access policy that has session controls for Microsoft SharePoint Online.
Control privileged access to applications by using access reviews in Azure AD.
Requirements. Monitoring Requirements
Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged attacks that include a combination of

suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity. Question HOTSPOT -
You need to configure app registration in Azure AD to meet the delegation requirements.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:



Answer:



Explanation:

For both questions see URL provide in answer section of question;

https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-app-roles#restrict-who-can-create-applications

and extraction from URL's

#1 "On the User settings page for your organization, set the Users can register applications setting to No. This will disable the default ability for users to create application registrations."

#2 "By default in Azure AD, all users can register applications and manage all aspects of applications they create. Everyone also has the ability to consent to apps accessing company data on their behalf. You can choose to selectively grant those permissions by setting the global switches to 'No' and adding the selected users to the Application Developer role."

These meet question answers

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-app-roles

Question: 301 CertyIQ

Introductory Info Case Study -

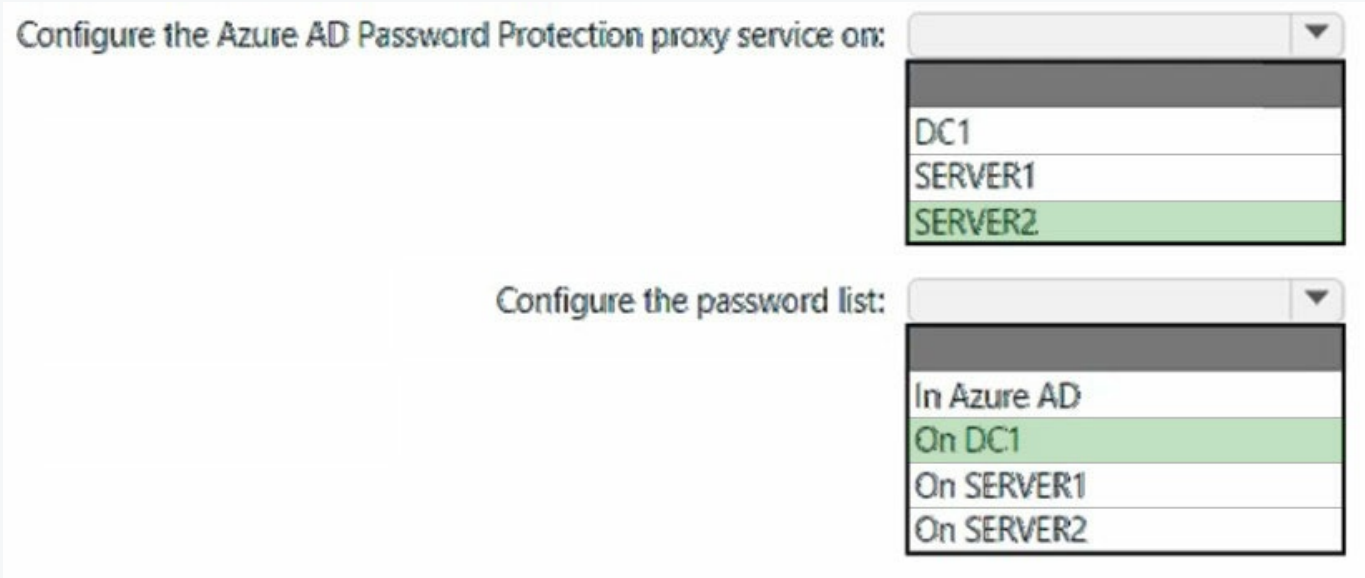
Overview -
Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.
Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.
Existing Environment. Identity Environment
The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD
Connect uses pass-through authentication and has password hash synchronization disabled.
Litware.com contains a user named User1 who oversees all application development.
Litware implements Azure AD Application Proxy.
Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.
Existing Environment. Cloud Environment
All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.
Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active
Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.
Existing Environment. On-premises Environment
The on-premises network contains the servers shown in the following table.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller for litware.com
SERVER1	Windows Server 2019	Boston	Member server in litware.com that runs the Azure AD Application Proxy connector
SERVER2	Windows Server 2019	Boston	Member server that uses Azure AD Connect

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.
Requirements. Delegation Requirements
Litware identifies the following delegation requirements:
Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).
Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.
Use custom programs for Identity Governance.
Ensure that User1 can create enterprise applications in Azure AD.
Use the principle of least privilege.
Requirements. Licensing Requirements
Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest.
Litware wants to manage the assignment of Azure
AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to a
Microsoft 365 group that has the appropriate licenses assigned.
Requirements. Management Requirements
Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.
Requirements. Authentication Requirements
Litware identifies the following authentication requirements:
Implement multi-factor authentication (MFA) for all Litware users by using conditional access policies.
Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.
Implement a banned password list for the litware.com forest.
Enforce MFA when accessing on-premises applications.
Automatically detect and remediate externally leaked credentials.
Requirements. Access Requirements

Litware identifies the following access requirements:
Control all access to all Azure resources and Azure AD applications by using conditional access policies.
Implement a conditional access policy that has session controls for Microsoft SharePoint Online.
Control privileged access to applications by using access reviews in Azure AD.
Requirements. Monitoring Requirements
Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged attacks that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity. Question HOTSPOT -
How should the access be setup to the on-premises applications?
Hot Area:

Answer:



Explanation:
Box 1: Server2 -
Incorrect:
Not Server 1: If you've deployed Azure AD Password Protection Proxy, do not install Azure AD Application Proxy and Azure AD Password Protection Proxy together on the same machine. Azure AD Application Proxy and Azure AD Password Protection Proxy install different versions of the Azure AD Connect Agent Updater service. These different versions are incompatible when installed together on the same machine.
Server1 runs the Azure AD application Proxy connector.
To use Application Proxy, you need a Windows server running Windows Server 2012 R2 or later. You'll install the Application Proxy connector on the server. This connector server needs to connect to the Application Proxy services in Azure, and the on-premises applications that you plan to publish.
Scenario:
Requirements. Authentication Requirements include:

Enforce MFA when accessing on-premises applications.
Existing Environment. On-premises Environment
The on-premises network contains the servers shown in the following table.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller for litware.com
SERVER1	Windows Server 2019	Boston	Member server in litware.com that runs the Azure AD Application Proxy connector
SERVER2	Windows Server 2019	Boston	Member server that uses Azure AD Connect

Existing Environment. Identity Environment
The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD
Connect uses pass-through authentication and has password hash synchronization disabled.
Litware.com contains a user named User1 who oversees all application development.

Box 2: DC1 -
The Azure AD Password Protection proxy service is typically on a member server in your on-premises AD DS environment. Once installed, the Azure AD
Password Protection proxy service communicates with Azure AD to maintain a copy of the global and customer banned password lists for your Azure AD tenant.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-deploy https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-add-on-premises-application

Question: 302 CertyIQ

Introductory Info Case Study -

Overview -
Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle.
Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.
Existing Environment. Existing Environment
The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named
Contoso_Resources. The Contoso_Resources OU contains all users and computers.
The contoso.com Active Directory domain contains the relevant users shown in the following table.

Name	Office	Department
Admin1	Montreal	Helpdesk
User1	Montreal	HR
User2	Montreal	HR
User3	Montreal	HR
Admin2	London	Helpdesk
User4	London	Finance
User5	London	Sales
User6	London	Sales
Admin3	Seattle	Helpdesk
User7	Seattle	Sales
User8	Seattle	Sales
User9	Seattle	Sales

Contoso also includes a marketing department that has users in each office.
Existing Environment. Microsoft 365/Azure Environment
Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:
Microsoft Office 365 Enterprise E5
Enterprise Mobility + Security E5
Windows 10 Enterprise E3
Project Plan 3
Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso_Resources OU is synced.
Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.
User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:
The users in the London office have the Microsoft 365 Phone System license unassigned.
The users in the Seattle office have the Yammer Enterprise license unassigned.
Security defaults are disabled for contoso.com.
Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.
Existing Environment. Problem Statements
Contoso identifies the following issues:
Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.
The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.
The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.
Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.
When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes -
Contoso plans to implement the following changes:
Implement self-service password reset (SSPR).
Analyze Azure audit activity logs by using Azure Monitor.
Simplify license allocation for new users added to the tenant.
Collaborate with the users at Fabrikam on a joint marketing campaign.
Configure the User administrator role to require justification and approval to activate.
Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.
For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.
Contoso plans to acquire a company named ADatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.
Requirements. Technical Requirements
Contoso identifies the following technical requirements:
All users must be synced from AD DS to the contoso.com Azure AD tenant.
App1 must have a redirect URI pointed to https://contoso.com/auth-response.

License allocation for new users must be assigned automatically based on the location of the user.
Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.
Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.
The helpdesk administrators must be able to manage licenses for only the users in their respective office.
Users must be forced to change their password if there is a probability that the users' identity was compromised.
Question You create a Log Analytics workspace.
You need to implement the technical requirements for auditing.
What should you configure in Azure AD?

A. Company branding
B. Diagnostics settings
C. External Identities
D. App registrations

Answer: B

Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/overview-monitoring

Question: 303 CertyIQ

Introductory Info Case Study -

Overview -
Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle.
Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.
Existing Environment. Existing Environment
The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named
Contoso_Resources. The Contoso_Resources OU contains all users and computers.
The contoso.com Active Directory domain contains the relevant users shown in the following table.

Name	Office	Department
Admin1	Montreal	Helpdesk
User1	Montreal	HR
User2	Montreal	HR
User3	Montreal	HR
Admin2	London	Helpdesk
User4	London	Finance
User5	London	Sales
User6	London	Sales
Admin3	Seattle	Helpdesk
User7	Seattle	Sales
User8	Seattle	Sales
User9	Seattle	Sales

Contoso also includes a marketing department that has users in each office.
Existing Environment. Microsoft 365/Azure Environment
Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:
Microsoft Office 365 Enterprise E5
Enterprise Mobility + Security E5
Windows 10 Enterprise E3

Project Plan 3
Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso_Resources OU is synced.
Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.
User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:
The users in the London office have the Microsoft 365 Phone System license unassigned.
The users in the Seattle office have the Yammer Enterprise license unassigned.
Security defaults are disabled for contoso.com.
Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.
Existing Environment. Problem Statements
Contoso identifies the following issues:
Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.
The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.
The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.
Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.
When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes -
Contoso plans to implement the following changes:
Implement self-service password reset (SSPR).
Analyze Azure audit activity logs by using Azure Monitor.
Simplify license allocation for new users added to the tenant.
Collaborate with the users at Fabrikam on a joint marketing campaign.
Configure the User administrator role to require justification and approval to activate.
Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.
For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.
Contoso plans to acquire a company named ADatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.
Requirements. Technical Requirements
Contoso identifies the following technical requirements:
All users must be synced from AD DS to the contoso.com Azure AD tenant.
App1 must have a redirect URI pointed to https://contoso.com/auth-response.
License allocation for new users must be assigned automatically based on the location of the user.
Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.
Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.
The helpdesk administrators must be able to manage licenses for only the users in their respective office.
Users must be forced to change their password if there is a probability that the users' identity was compromised.
Question HOTSPOT -
You need to implement the planned changes and technical requirements for the marketing department.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

To configure user access:

- An access package
- An access review
- A conditional access policy

To enable collaboration with fabrikam.com:

- An accepted domain
- A connected organization
- A custom domain name

Answer:

Answer Area

To configure user access: **An access package**

To enable collaboration with fabrikam.com: **A connected organization**

Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-organization

Question: 304 CertyIQ

Introductory Info Case Study -

Overview -
Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle. Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.
Existing Environment. Existing Environment
The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain

contains an organizational unit (OU) named
Contoso_Resources. The Contoso_Resources OU contains all users and computers.
The contoso.com Active Directory domain contains the relevant users shown in the following table.

Name	Office	Department
Admin1	Montreal	Helpdesk
User1	Montreal	HR
User2	Montreal	HR
User3	Montreal	HR
Admin2	London	Helpdesk
User4	London	Finance
User5	London	Sales
User6	London	Sales
Admin3	Seattle	Helpdesk
User7	Seattle	Sales
User8	Seattle	Sales
User9	Seattle	Sales

Contoso also includes a marketing department that has users in each office.
Existing Environment. Microsoft 365/Azure Environment
Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:
Microsoft Office 365 Enterprise E5
Enterprise Mobility + Security E5
Windows 10 Enterprise E3
Project Plan 3
Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso_Resources OU is synced.
Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.
User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:
The users in the London office have the Microsoft 365 Phone System license unassigned.
The users in the Seattle office have the Yammer Enterprise license unassigned.
Security defaults are disabled for contoso.com.
Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.
Existing Environment. Problem Statements
Contoso identifies the following issues:
Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.
The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.
The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.
Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.
When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes -
Contoso plans to implement the following changes:
Implement self-service password reset (SSPR).
Analyze Azure audit activity logs by using Azure Monitor.
Simplify license allocation for new users added to the tenant.
Collaborate with the users at Fabrikam on a joint marketing campaign.
Configure the User administrator role to require justification and approval to activate.
Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.
For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.
Contoso plans to acquire a company named ADatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.
Requirements. Technical Requirements

Contoso identifies the following technical requirements:
All users must be synced from AD DS to the contoso.com Azure AD tenant.
App1 must have a redirect URI pointed to https://contoso.com/auth-response.
License allocation for new users must be assigned automatically based on the location of the user.
Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.
Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.
The helpdesk administrators must be able to manage licenses for only the users in their respective office.
Users must be forced to change their password if there is a probability that the users' identity was compromised.
Question You need to meet the planned changes for the User administrator role.
What should you do?

A. Create an access review.
B. Create an administrative unit.
C. Modify Active assignments.
D. Modify Role settings.

Answer: D

Explanation:

Role Setting details is where you need to be: Role setting details - User Administrator

Privileged Identity Management | Azure AD roles

Default Setting State

Require justification on activation Yes

Require ticket information on activation No

On activation, require Azure MFA Yes

Require approval to activate No

Approvers None

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-add-role-to-user?tabs=new

Question: 305

CertyIQ

Introductory Info Case Study -

Overview -
Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle.
Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.
Existing Environment. Existing Environment
The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named
Contoso_Resources. The Contoso_Resources OU contains all users and computers.
The contoso.com Active Directory domain contains the relevant users shown in the following table.

Name	Office	Department
Admin1	Montreal	Helpdesk
User1	Montreal	HR
User2	Montreal	HR
User3	Montreal	HR
Admin2	London	Helpdesk
User4	London	Finance
User5	London	Sales
User6	London	Sales
Admin3	Seattle	Helpdesk
User7	Seattle	Sales
User8	Seattle	Sales
User9	Seattle	Sales

Contoso also includes a marketing department that has users in each office.
Existing Environment. Microsoft 365/Azure Environment
Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:
Microsoft Office 365 Enterprise E5
Enterprise Mobility + Security E5
Windows 10 Enterprise E3
Project Plan 3
Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso_Resources OU is synced.
Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.
User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:
The users in the London office have the Microsoft 365 Phone System license unassigned.
The users in the Seattle office have the Yammer Enterprise license unassigned.
Security defaults are disabled for contoso.com.
Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.
Existing Environment. Problem Statements
Contoso identifies the following issues:
Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.
The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.
The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.
Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.
When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes -
Contoso plans to implement the following changes:
Implement self-service password reset (SSPR).
Analyze Azure audit activity logs by using Azure Monitor.
Simplify license allocation for new users added to the tenant.
Collaborate with the users at Fabrikam on a joint marketing campaign.
Configure the User administrator role to require justification and approval to activate.
Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.
For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.
Contoso plans to acquire a company named ADatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.
Requirements. Technical Requirements
Contoso identifies the following technical requirements:
All users must be synced from AD DS to the contoso.com Azure AD tenant.
App1 must have a redirect URI pointed to https://contoso.com/auth-response.

License allocation for new users must be assigned automatically based on the location of the user.
Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.
Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.
The helpdesk administrators must be able to manage licenses for only the users in their respective office.
Users must be forced to change their password if there is a probability that the users' identity was compromised.
Question You need to modify the settings of the User administrator role to meet the technical requirements.
Which two actions should you perform for the role? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Select Require justification on activation.
B. Select Require ticket information on activation.
C. Modify the Expire eligible assignments after setting.
D. Set all assignments to Eligible.
E. Set all assignments to Active.

Answer: AD

Explanation:

To require justification need assignment to be Eligible instead of Active

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

Question: 306 CertyIQ

Introductory Info Case Study -

Overview -
Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle.
Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.
Existing Environment. Existing Environment
The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named
Contoso_Resources. The Contoso_Resources OU contains all users and computers.
The contoso.com Active Directory domain contains the relevant users shown in the following table.

Name	Office	Department
Admin1	Montreal	Helpdesk
User1	Montreal	HR
User2	Montreal	HR
User3	Montreal	HR
Admin2	London	Helpdesk
User4	London	Finance
User5	London	Sales
User6	London	Sales
Admin3	Seattle	Helpdesk
User7	Seattle	Sales
User8	Seattle	Sales
User9	Seattle	Sales

Contoso also includes a marketing department that has users in each office.
Existing Environment. Microsoft 365/Azure Environment
Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:

Microsoft Office 365 Enterprise E5
Enterprise Mobility + Security E5
Windows 10 Enterprise E3
Project Plan 3
Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso_Resources OU is synced.
Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.
User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:
The users in the London office have the Microsoft 365 Phone System license unassigned.
The users in the Seattle office have the Yammer Enterprise license unassigned.
Security defaults are disabled for contoso.com.
Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.
Existing Environment. Problem Statements
Contoso identifies the following issues:
Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.
The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.
The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.
Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.
When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes -
Contoso plans to implement the following changes:
Implement self-service password reset (SSPR).
Analyze Azure audit activity logs by using Azure Monitor.
Simplify license allocation for new users added to the tenant.
Collaborate with the users at Fabrikam on a joint marketing campaign.
Configure the User administrator role to require justification and approval to activate.
Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.
For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.
Contoso plans to acquire a company named ADatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.
Requirements. Technical Requirements
Contoso identifies the following technical requirements:
All users must be synced from AD DS to the contoso.com Azure AD tenant.
App1 must have a redirect URI pointed to https://contoso.com/auth-response.
License allocation for new users must be assigned automatically based on the location of the user.
Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.
Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.
The helpdesk administrators must be able to manage licenses for only the users in their respective office.
Users must be forced to change their password if there is a probability that the users' identity was compromised.
Question You need to resolve the issue of the guest user invitations.
What should you do for the Azure AD tenant?

A. Configure the Continuous access evaluation settings.
B. Configure a Conditional Access policy.
C. Configure the Access reviews settings.
D. Modify the External collaboration settings.

Answer: D

Explanation:

"You need to resolve the issue of the guest user invitations." Guest user invitations is the key.

Invitation settings are in "External collaboration settings" blade.

You can allow anyone in the organization to invite guest users, or restrict it to the specific admin role and grant users permission to the Guest Inviter role.

Access reviews have nothing in common with user invitations.

I would think the guest user issue that needs resolving would be: "Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days". If that is the case answer should be D.

Question: 307 CertyIQ

Introductory Info Case Study -

Overview -
Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle.
Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.
Existing Environment. Existing Environment
The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named
Contoso_Resources. The Contoso_Resources OU contains all users and computers.
The contoso.com Active Directory domain contains the relevant users shown in the following table.

Name	Office	Department
Admin1	Montreal	Helpdesk
User1	Montreal	HR
User2	Montreal	HR
User3	Montreal	HR
Admin2	London	Helpdesk
User4	London	Finance
User5	London	Sales
User6	London	Sales
Admin3	Seattle	Helpdesk
User7	Seattle	Sales
User8	Seattle	Sales
User9	Seattle	Sales

Contoso also includes a marketing department that has users in each office.
Existing Environment. Microsoft 365/Azure Environment
Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:
Microsoft Office 365 Enterprise E5
▪
Enterprise Mobility + Security E5
Windows 10 Enterprise E3
Project Plan 3
Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso_Resources OU is synced.
Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.
User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:
The users in the London office have the Microsoft 365 Phone System license unassigned.
The users in the Seattle office have the Yammer Enterprise license unassigned.
Security defaults are disabled for contoso.com.
Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.
Existing Environment. Problem Statements
Contoso identifies the following issues:
Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.
The user administrators report that it is tedious to manually configure the different license requirements for each

Contoso office.
The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.
Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.
When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes -
Contoso plans to implement the following changes:
Implement self-service password reset (SSPR).
Analyze Azure audit activity logs by using Azure Monitor.
Simplify license allocation for new users added to the tenant.
Collaborate with the users at Fabrikam on a joint marketing campaign.
Configure the User administrator role to require justification and approval to activate.
Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.
For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.
Contoso plans to acquire a company named ADatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.
Requirements. Technical Requirements
Contoso identifies the following technical requirements:
All users must be synced from AD DS to the contoso.com Azure AD tenant.
App1 must have a redirect URI pointed to https://contoso.com/auth-response.
License allocation for new users must be assigned automatically based on the location of the user.
Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.
Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.
The helpdesk administrators must be able to manage licenses for only the users in their respective office.
Users must be forced to change their password if there is a probability that the users' identity was compromised.
Question You need to sync the ADatum users. The solution must meet the technical requirements.
What should you do?

A. From the Microsoft Azure Active Directory Connect wizard, select Customize synchronization options.
B. From PowerShell, run Set-ADSyncScheduler.
C. From PowerShell, run Start-ADSyncSyncCycle.
D. From the Microsoft Azure Active Directory Connect wizard, select Change user sign-in.

Answer: A

Explanation:

You need to select Customize synchronization options to configure Azure AD Connect to sync the Adatum organizational unit (OU).

Answer A is correct.

The following link gets to the point.

https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering#filtering-options

Gives more info.

https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-whatis#azure-ad-connect-sync-topics

Question: 308

Introductory Info Case Study -

Overview -
Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.
Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.
Existing Environment. Identity Environment
The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD
Connect uses pass-through authentication and has password hash synchronization disabled.
Litware.com contains a user named User1 who oversees all application development.
Litware implements Azure AD Application Proxy.
Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.
Existing Environment. Cloud Environment
All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.
Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active
Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.
Existing Environment. On-premises Environment
The on-premises network contains the servers shown in the following table.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller for litware.com
SERVER1	Windows Server 2019	Boston	Member server in litware.com that runs the Azure AD Application Proxy connector
SERVER2	Windows Server 2019	Boston	Member server that uses Azure AD Connect

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.
Requirements. Delegation Requirements
Litware identifies the following delegation requirements:
Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).
Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.
Use custom programs for Identity Governance.
Ensure that User1 can create enterprise applications in Azure AD.
Use the principle of least privilege.
Requirements. Licensing Requirements
Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest.
Litware wants to manage the assignment of Azure
AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to a
Microsoft 365 group that has the appropriate licenses assigned.
Requirements. Management Requirements
Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.
Requirements. Authentication Requirements
Litware identifies the following authentication requirements:
Implement multi-factor authentication (MFA) for all Litware users by using conditional access policies.
Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.
-
Implement a banned password list for the litware.com forest.
Enforce MFA when accessing on-premises applications.
Automatically detect and remediate externally leaked credentials.
Requirements. Access Requirements
Litware identifies the following access requirements:
Control all access to all Azure resources and Azure AD applications by using conditional access policies.
Implement a conditional access policy that has session controls for Microsoft SharePoint Online.

Control privileged access to applications by using access reviews in Azure AD.
Requirements. Monitoring Requirements
Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged attacks that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity. Question You need to configure the detection of multi-staged attacks to meet the monitoring requirements.
What should you do?

A. Customize the Microsoft Sentinel rule logic.
B. Create a workbook.
C. Add Microsoft Sentinel data connectors.
D. Add an Microsoft Sentinel playbook.

Answer: A

Explanation:

https://learn.microsoft.com/en-us/azure/sentinel/configure-fusion-rules#configure-fusion-rules

Question: 309 CertyIQ

Introductory Info Case Study -

Overview -
Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.
Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.
Existing Environment. Identity Environment
The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD
Connect uses pass-through authentication and has password hash synchronization disabled.
Litware.com contains a user named User1 who oversees all application development.
Litware implements Azure AD Application Proxy.
Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.
Existing Environment. Cloud Environment
All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.
Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active
Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.
Existing Environment. On-premises Environment
The on-premises network contains the servers shown in the following table.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller for litware.com
SERVER1	Windows Server 2019	Boston	Member server in litware.com that runs the Azure AD Application Proxy connector
SERVER2	Windows Server 2019	Boston	Member server that uses Azure AD Connect

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.
Requirements. Delegation Requirements

Litware identifies the following delegation requirements:
Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).
Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.
Use custom programs for Identity Governance.
Ensure that User1 can create enterprise applications in Azure AD.
Use the principle of least privilege.
Requirements. Licensing Requirements
Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest.
Litware wants to manage the assignment of Azure
AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to a
Microsoft 365 group that has the appropriate licenses assigned.
Requirements. Management Requirements
Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.
Requirements. Authentication Requirements
Litware identifies the following authentication requirements:
Implement multi-factor authentication (MFA) for all Litware users by using conditional access policies.
Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.
Implement a banned password list for the litware.com forest.
Enforce MFA when accessing on-premises applications.
Automatically detect and remediate externally leaked credentials.
Requirements. Access Requirements
Litware identifies the following access requirements:
Control all access to all Azure resources and Azure AD applications by using conditional access policies.
Implement a conditional access policy that has session controls for Microsoft SharePoint Online.
Control privileged access to applications by using access reviews in Azure AD.
Requirements. Monitoring Requirements
Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged attacks that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity. Question You need to track application access assignments by using Identity Governance. The solution must meet the delegation requirements.
What should you do first?

A. Modify the User consent settings for the enterprise applications.

B. Create a catalog.

C. Create a program.

D. Modify the Admin consent requests settings for the enterprise applications.

Answer: C

Explanation:

The Answer is C - Programs as stated they are requiring the use of custom programs

Litware identifies the following delegation requirements:

Use custom programs for Identity Governance.

Thank you

Thank you for being so interested in the premium exam material.
I'm glad to hear that you found it informative and helpful.

If you have any feedback or thoughts on the bumps, I would love to hear them.
Your insights can help me improve our writing and better understand our readers.

Best of Luck

You have worked hard to get to this point, and you are well-prepared for the exam
Keep your head up, stay positive, and go show that exam what you're made of!

Feedback

More Papers

Total: **309 Questions**

Link: https://certyiq.com/papers/microsoft/sc-300