Microsoft

(SC-300)

Microsoft Identity and Access Administrator

Total: **385 Questions**

Link:

Question: 1

You have an Azure Active Directory (Azure AD) tenant that contains the following objects:➪ A device named Device1
➪ Users named User1, User2, User3, User4, and User5
➪ Groups named Group1, Group2, Group3, Group4, and Group5
The groups are configured as shown in the following table.

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

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

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

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

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.

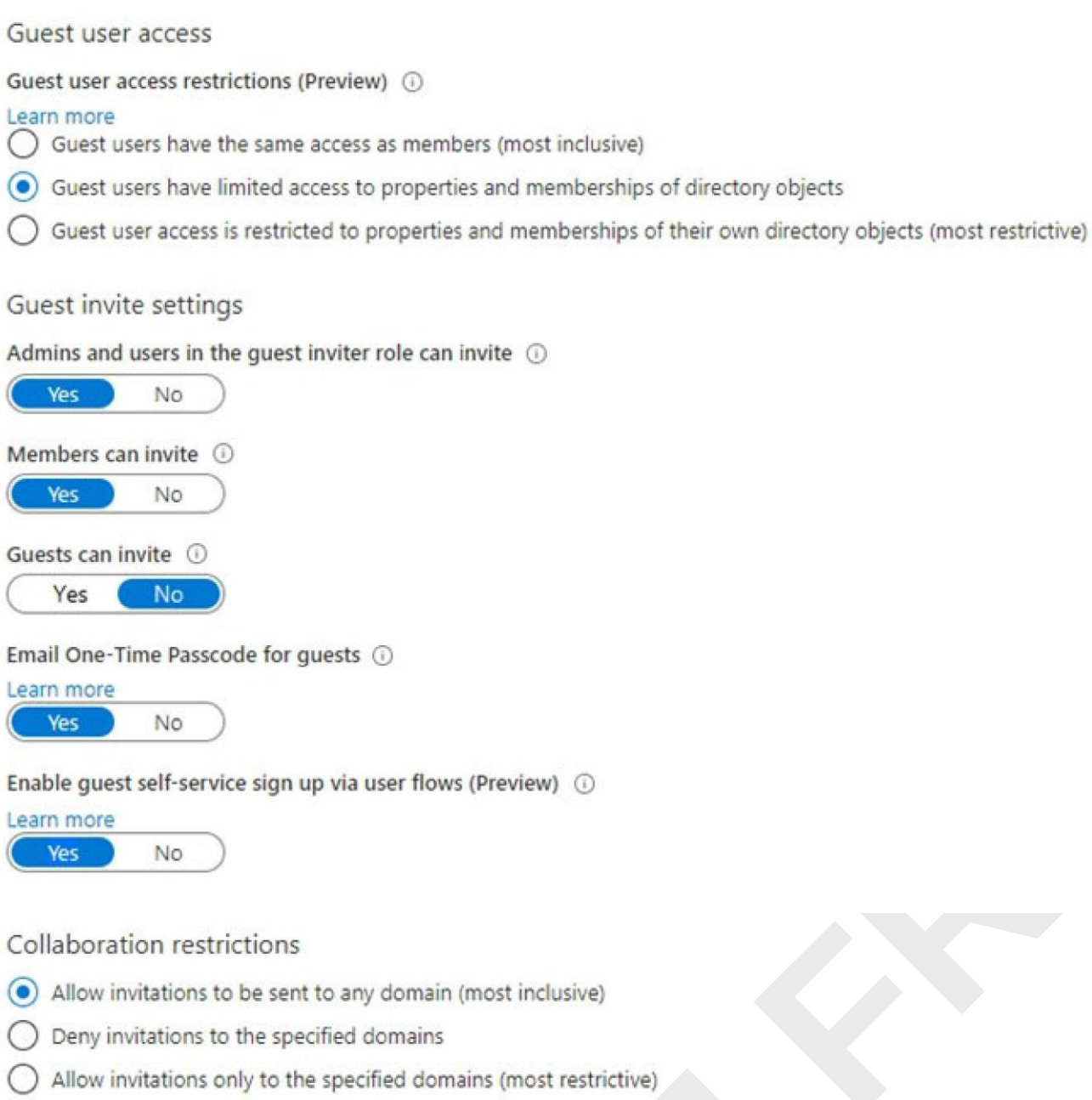
Azure AD cmdlet Set-MsolCompanySettings could help you to prevent creating user accounts with parameters:
AllowEmailVerifiedUsers (users can join the tenant by email validation)-->when is TRUE.

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 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

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

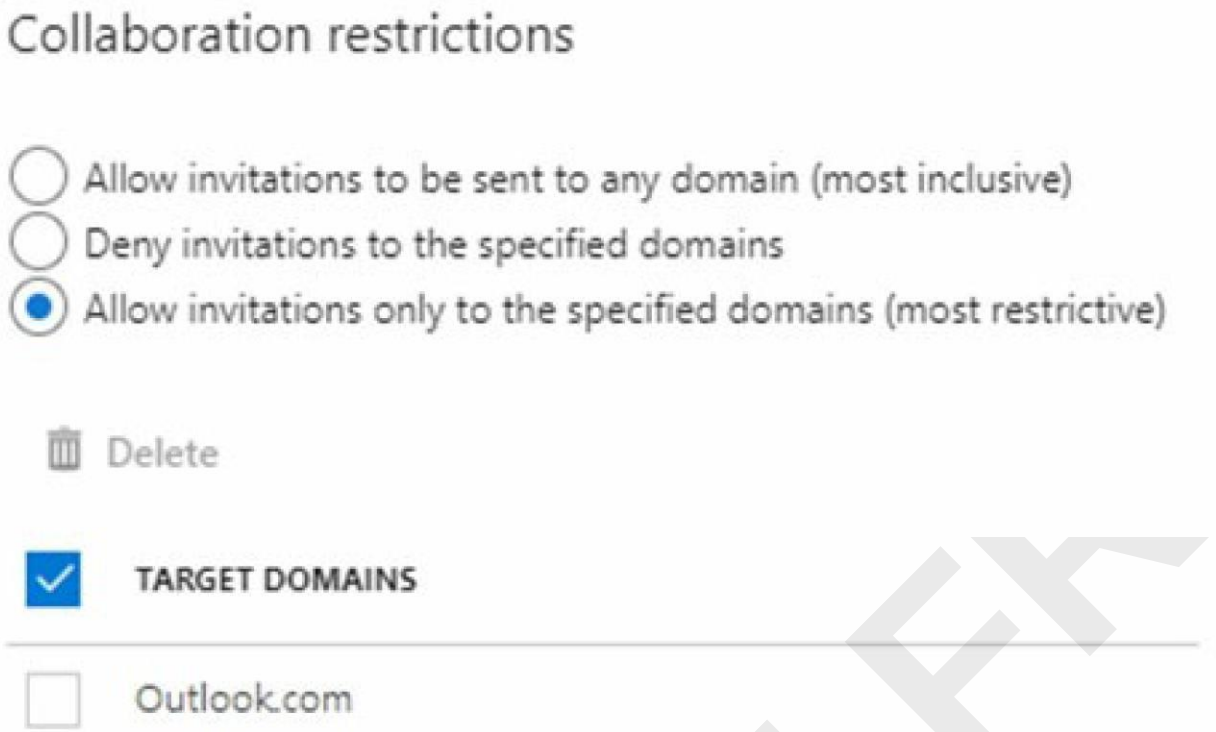
Reference:
https://docs.microsoft.com/en-us/microsoft-365/admin/manage/remove-licenses-from-users?view=o365-wor ldwide

Question: 5

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 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 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.

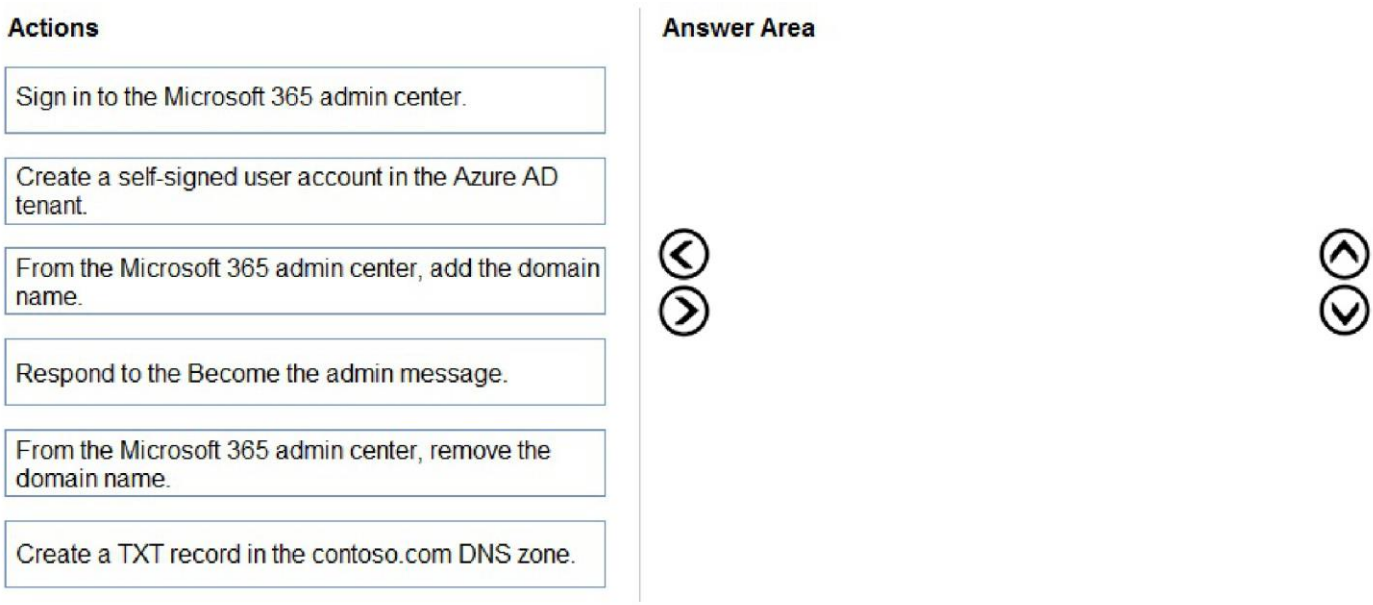
Question: 8 DRAG DROP -

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.

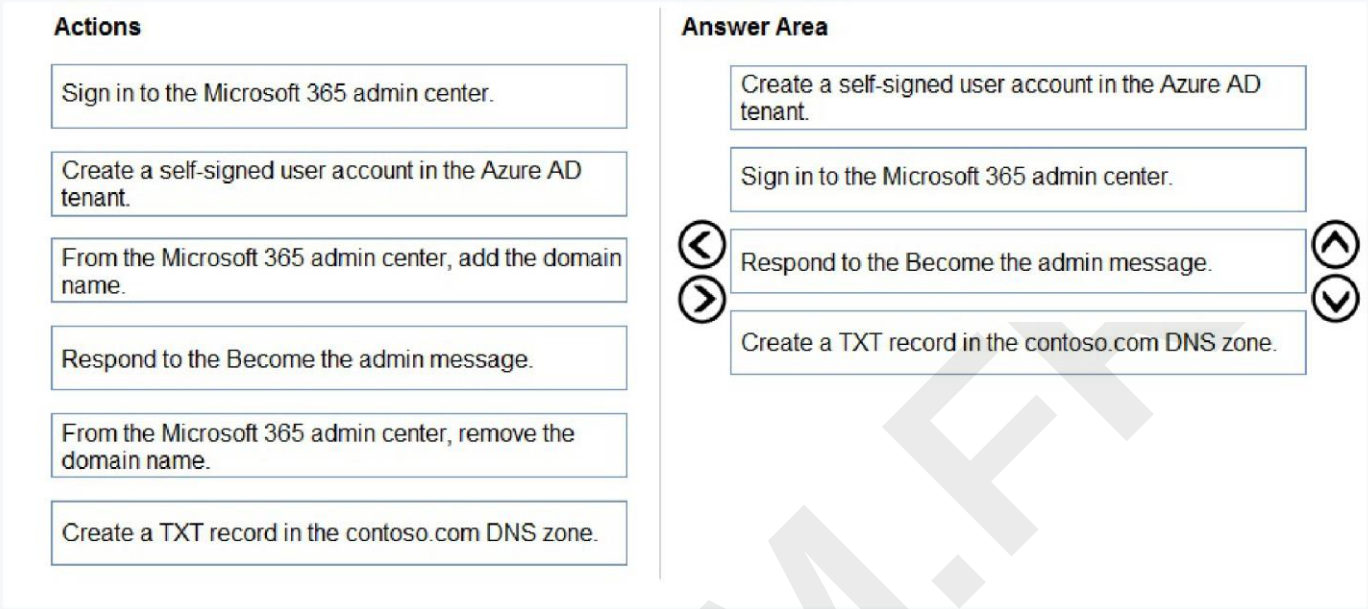
You need to gain global administrator privileges to the Azure Active Directory (Azure AD) tenant that contains the self-signed users.

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:



Answer:



Explanation:

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

Question: 9

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:

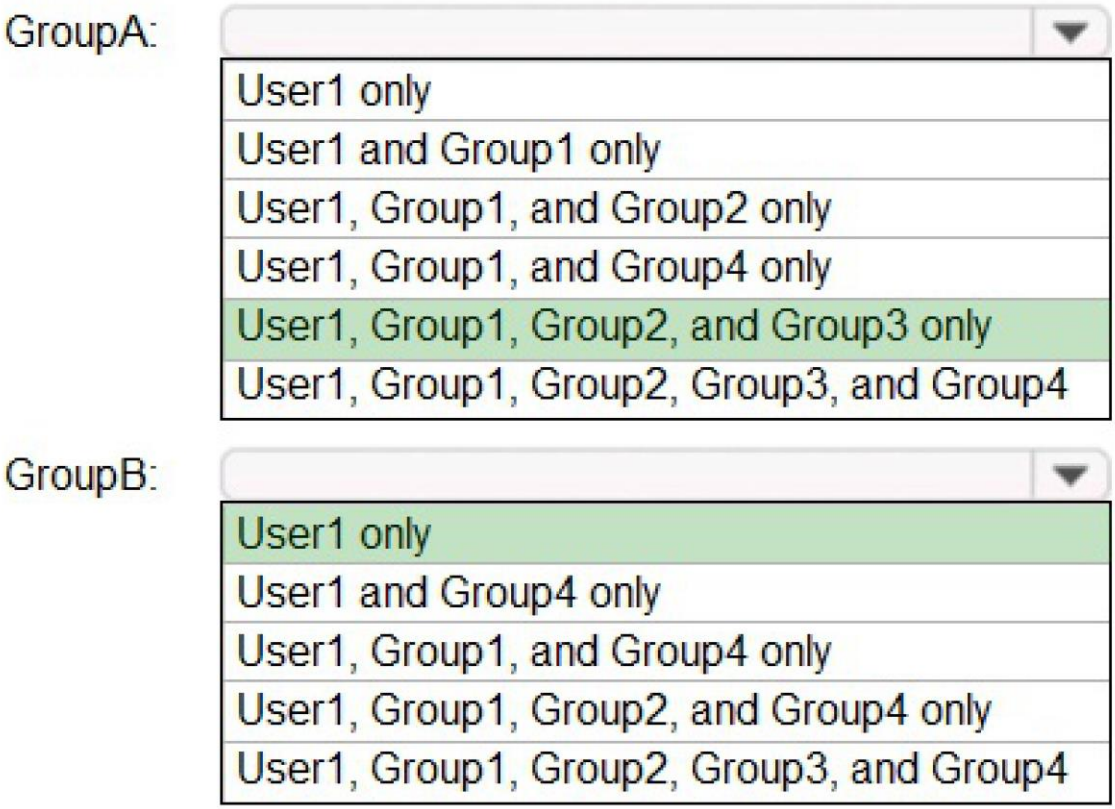
- User1 only
- User1 and Group1 only
- User1, Group1, and Group2 only
- User1, Group1, and Group4 only
- User1, Group1, Group2, and Group3 only
- User1, Group1, Group2, Group3, and Group4

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



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

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

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

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 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

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

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

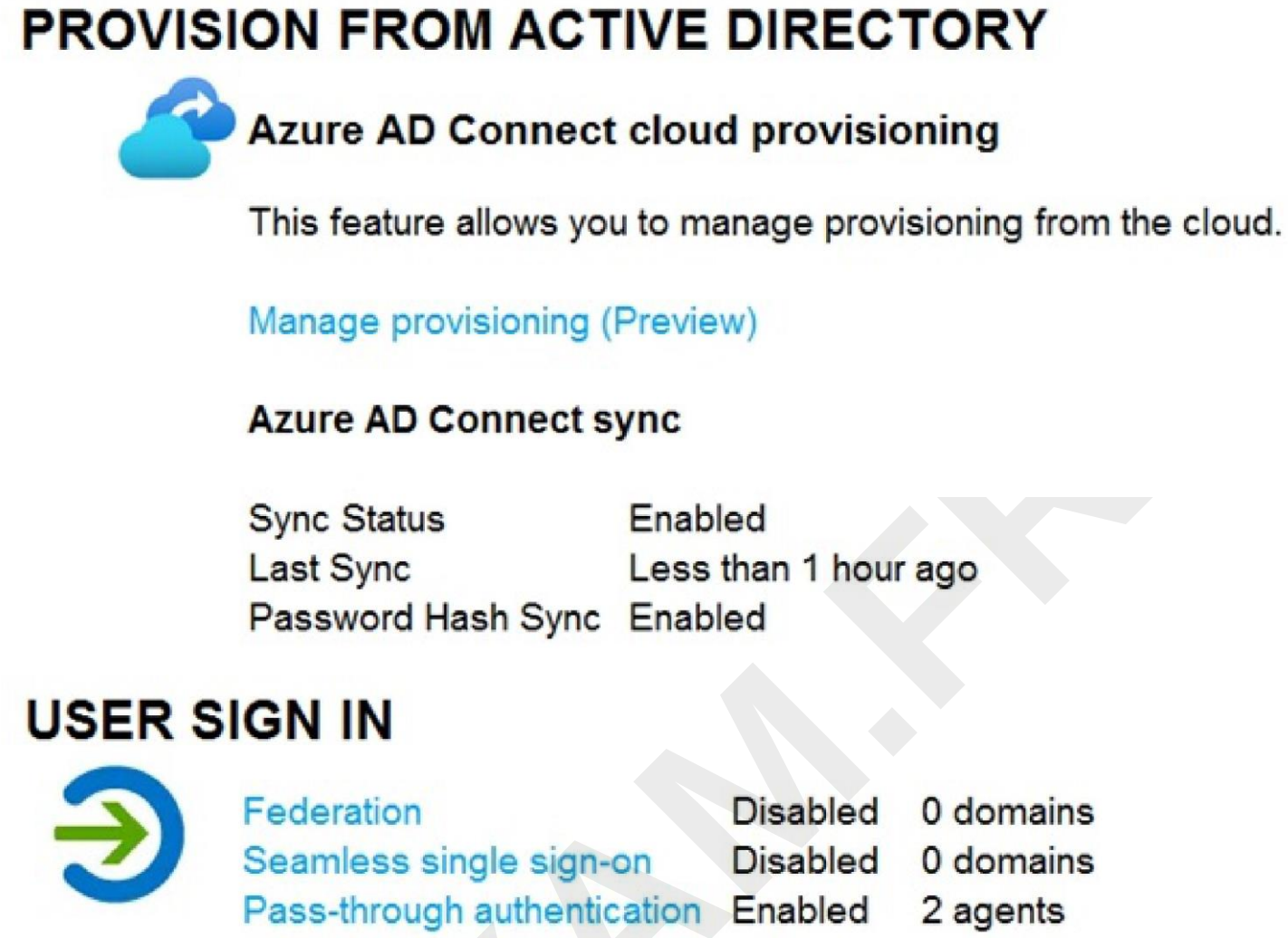
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-change-the-configuration

Question: 16

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

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.

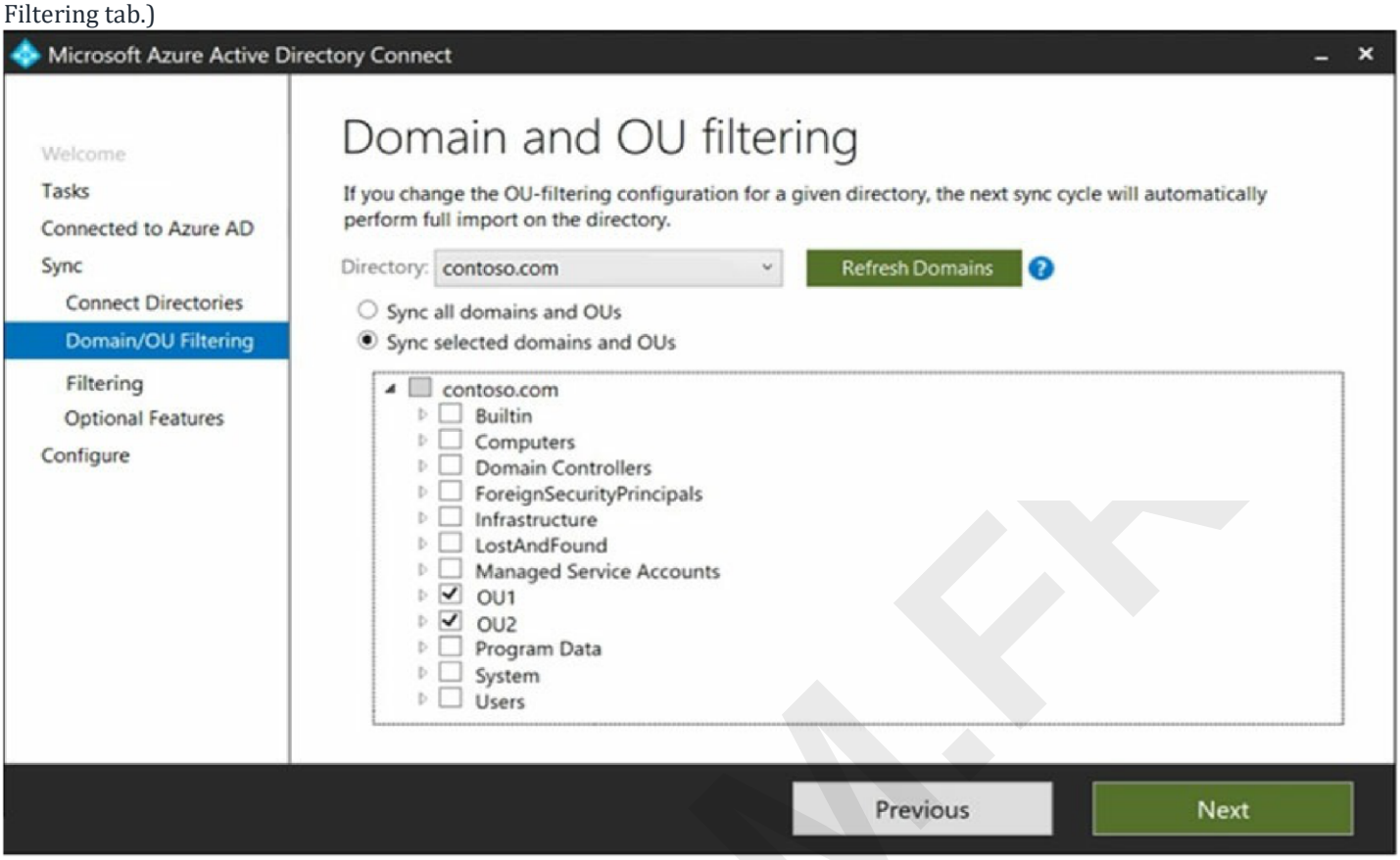
Azure Active Directory (Azure AD) Pass-through Authentication allows your users to sign in to both on-premises and cloud-based applications by using the same passwords. Pass-through Authentication signs users in by validating their passwords directly against on-premises Active Directory.

Question: 18

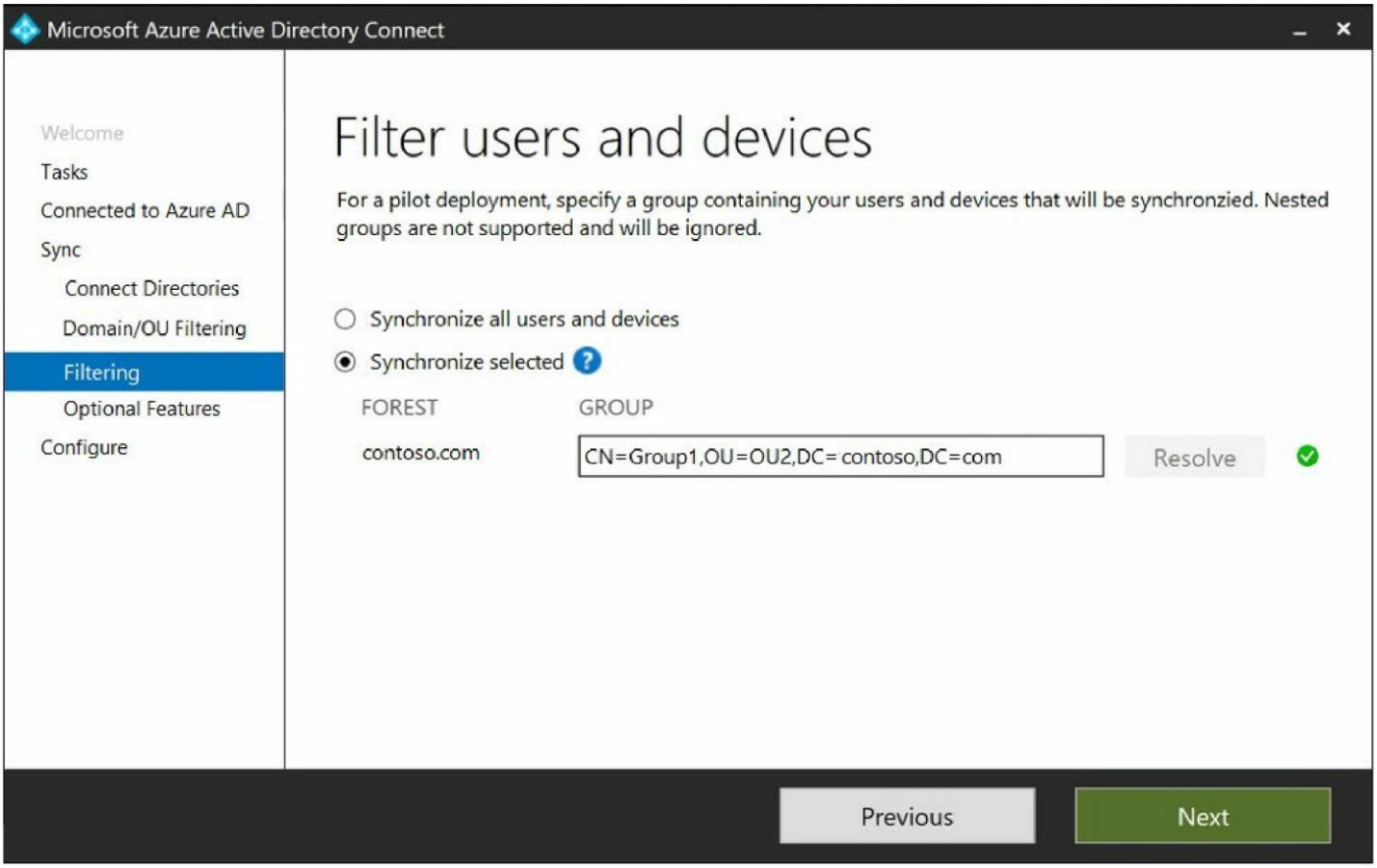
HOTSPOT -
Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the objects shown in the following table.

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

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

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:

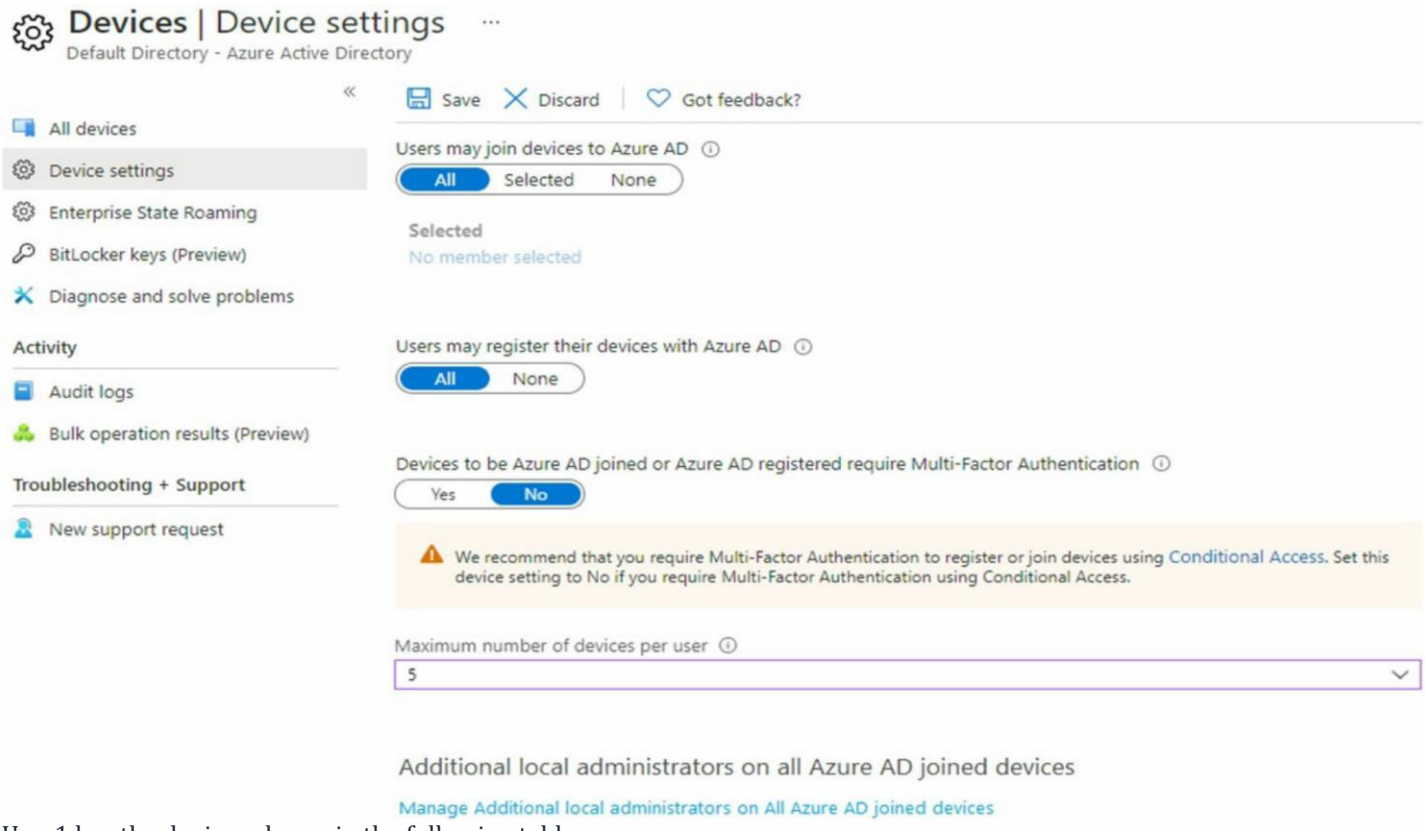
Reference:
https://practical365.com/configure-a-custom-domain-in-office-365/

Question: 21

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:

Box 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.

Box 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

Box 3: No -

An additional local device administrator has not been applied

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal#:~:text=Maximum%20number%20of%20devices%20setting%20applies%20to%20devices%20that%20are%

Question: 22 DRAG DROP -

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

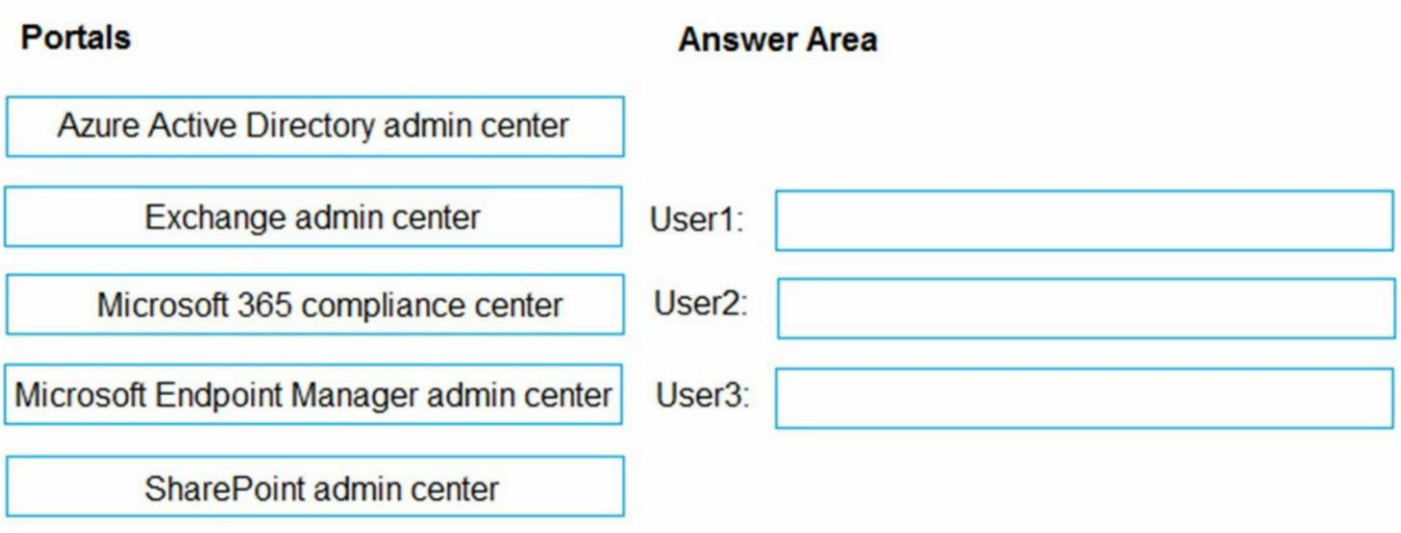
You need to configure the users as shown in the following table.

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

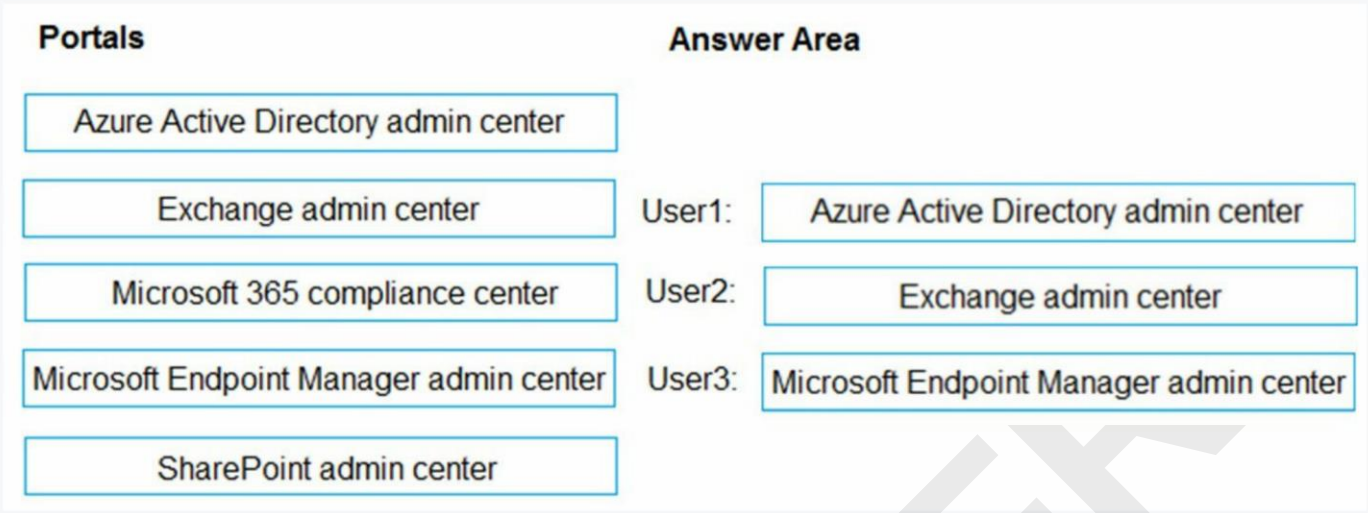
Which portal should you use to configure each user? To answer, drag the appropriate portals to the correct users. Each portal may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Answer:



Explanation:

Azure Active Directory admin center.

Exchange Admin center.

Microsoft Endpoint Manager admin center.

Question: 23 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

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

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

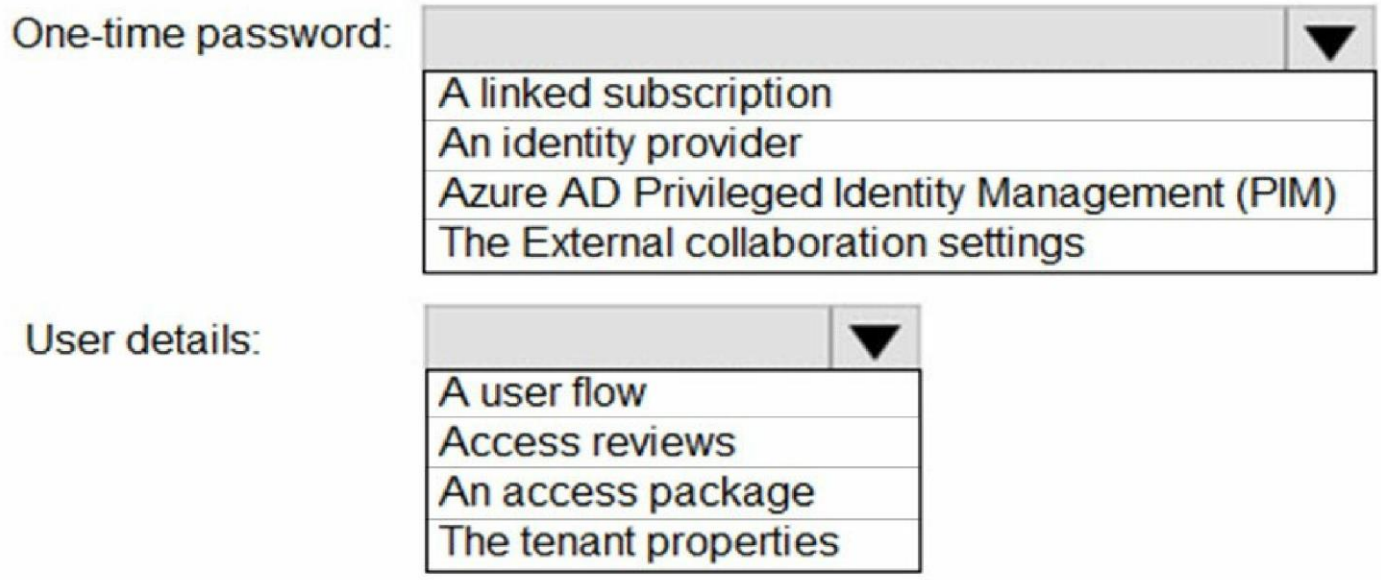
Explanation:
The Set-MsolUserLicense cmdlet updates the license assignment for a user. This can include adding a new license, removing a license, updating the license options, or any combination of these actions.
Note:
There are several versions of this question in the exam. The question has two possible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

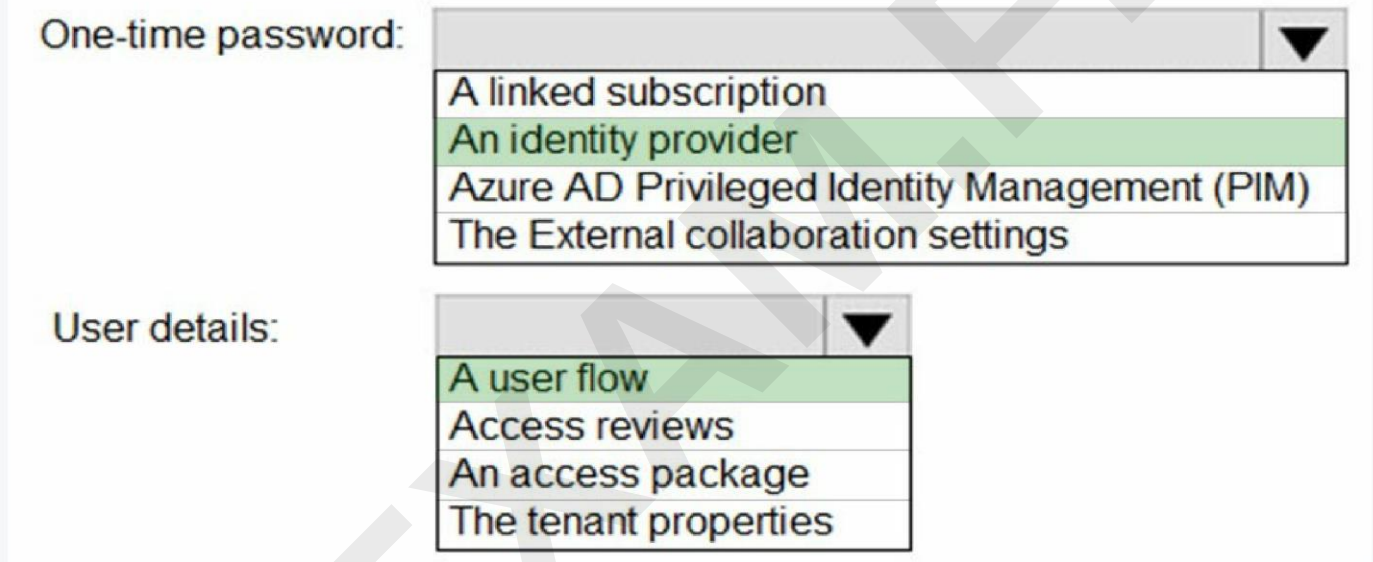
HOTSPOT -
You have an Azure Active Directory (Azure AD) tenant and an Azure web app named App1.
You need to provide guest users with self-service sign-up for App1. The solution must meet the following requirements:
☞ Guest users must be able to sign up by using a one-time password.
☞ The users must provide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

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

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 DRAG

DROP -

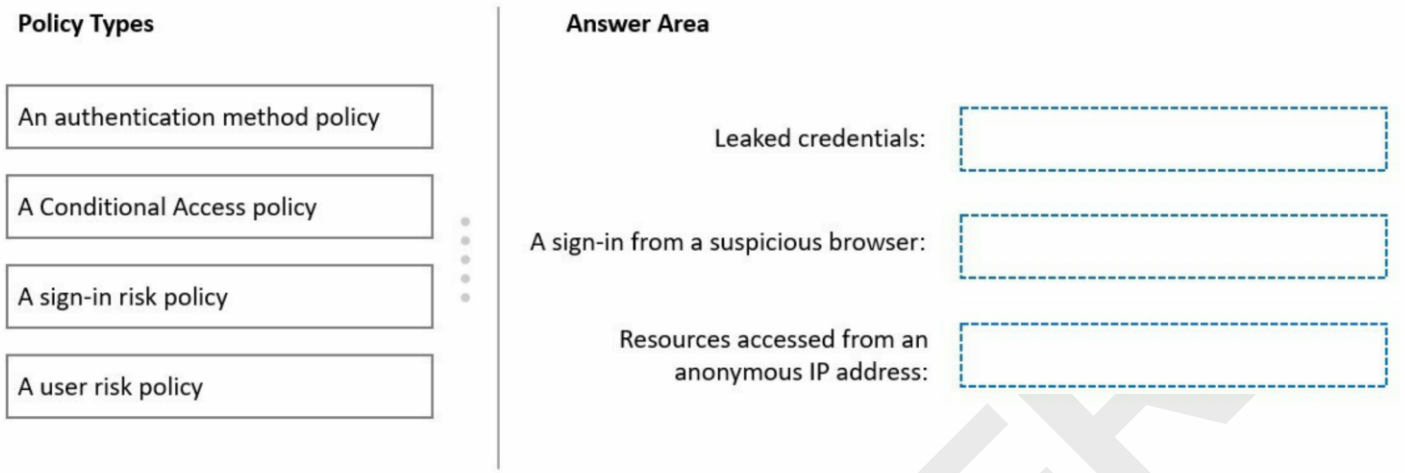
You need to resolve the recent security incident issues.

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

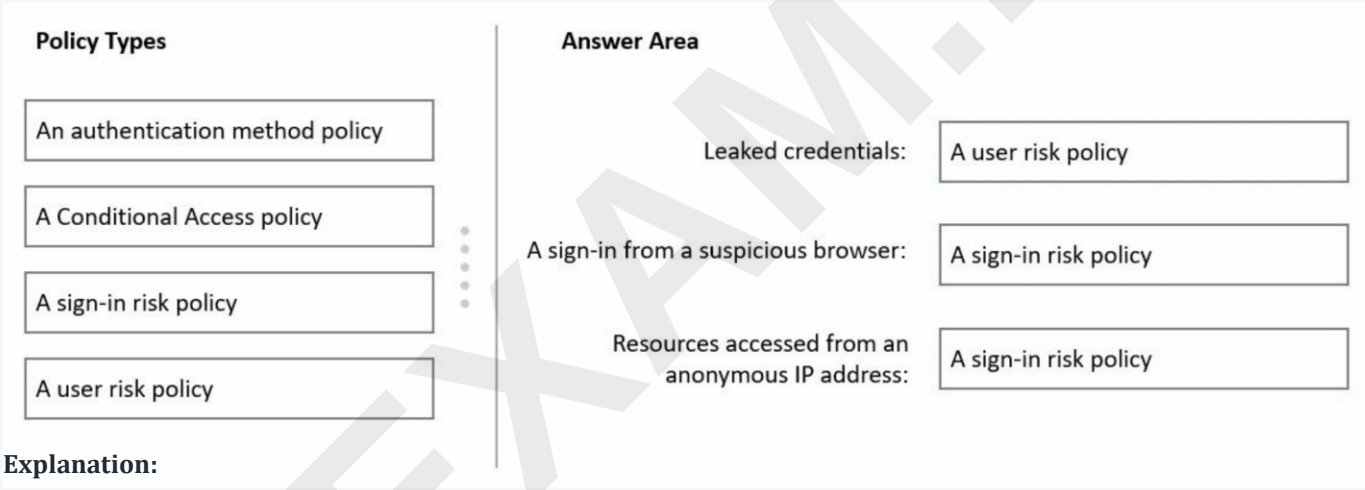
Each policy type may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

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

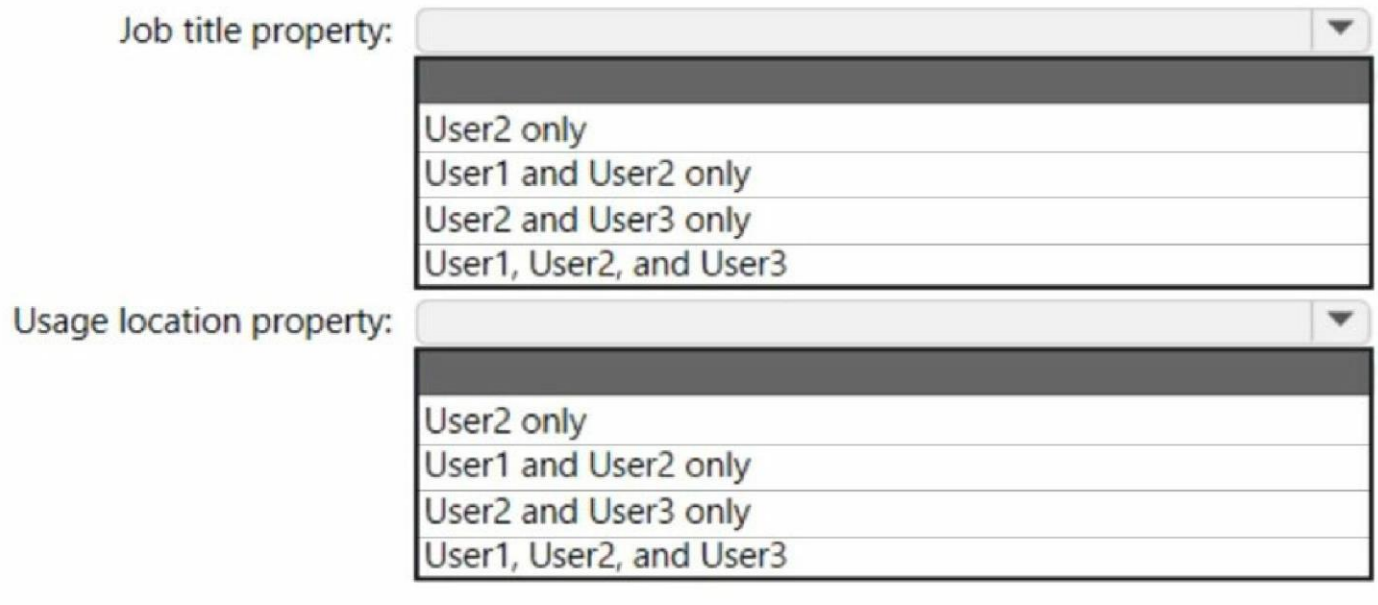
Question: 30 HOTSPOT

-

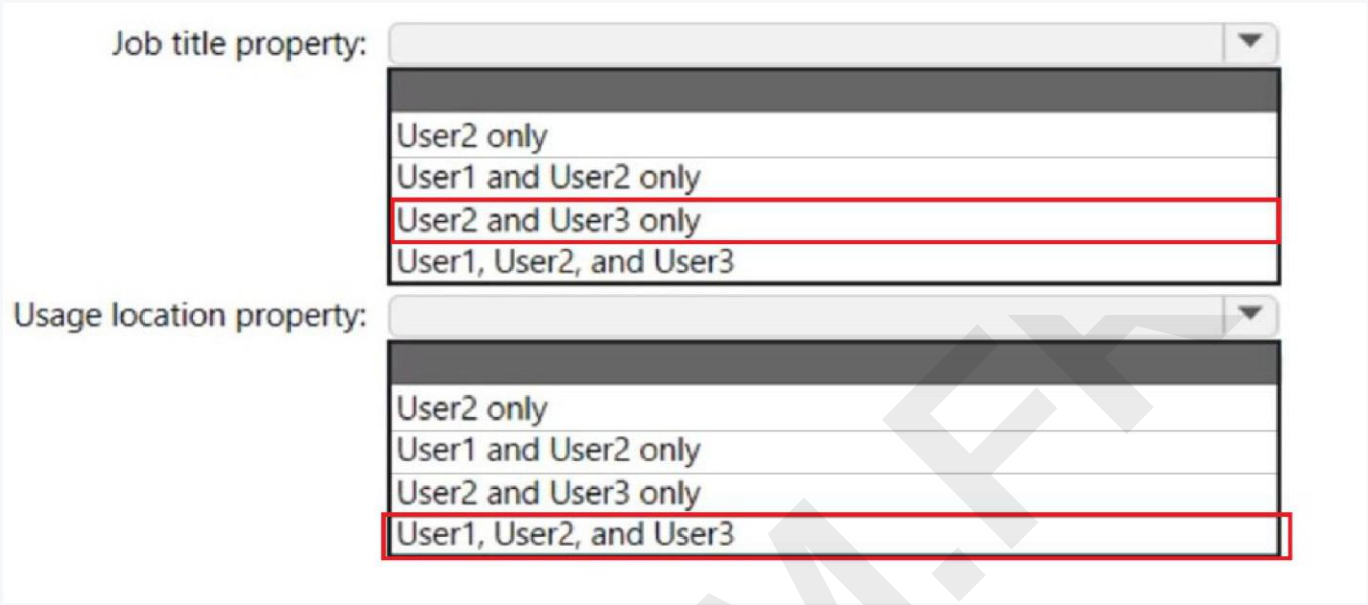
You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

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.

This selection likely applies a filter or condition that limits the scope of an operation, report, or policy to users who are associated with specific job titles.

"User2 and User3 only" restricts the operation to these users, possibly because their roles or responsibilities are relevant to the context being managed.

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.

Question: 31

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

Question: 32

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.

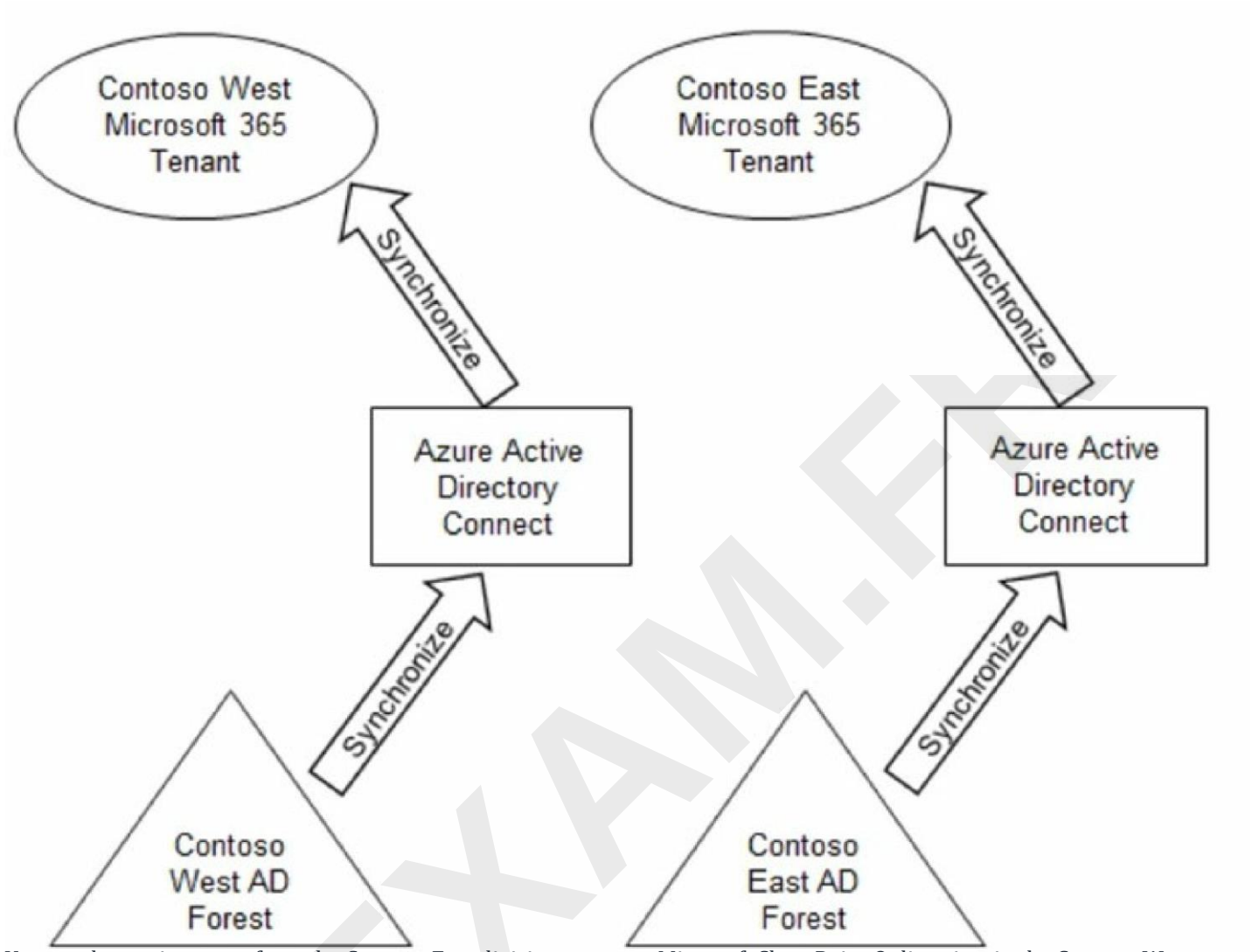
The catch is, "configure the Windows 10 computers.

The answer is C.

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

Question: 33

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

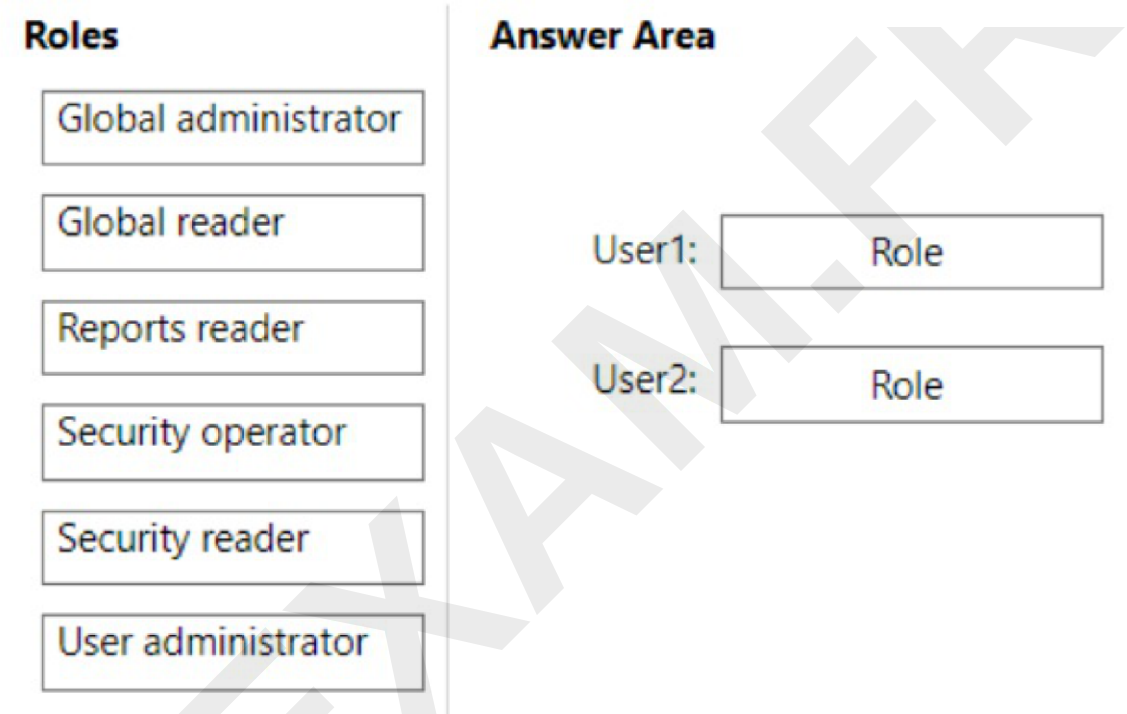
DRAG DROP
-

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:
User1: User Administrator.

"Create, update, or delete access review of a group or of an app" User2:
Security Reader.

"Read access review of a Microsoft Entra role"
Reference:
https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/delegate-by-task

Question: 35 HOTSPOT

-

You have an Azure subscription.

You need to create two custom roles named Role1 and Role2. The solution must meet the following requirements:• Users that are assigned Role1 can create or delete instances of Azure Container Apps.
• Users that are assigned Role2 can enforce adaptive network hardening rules.

Which resource provider permissions are required for each role? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Role1:

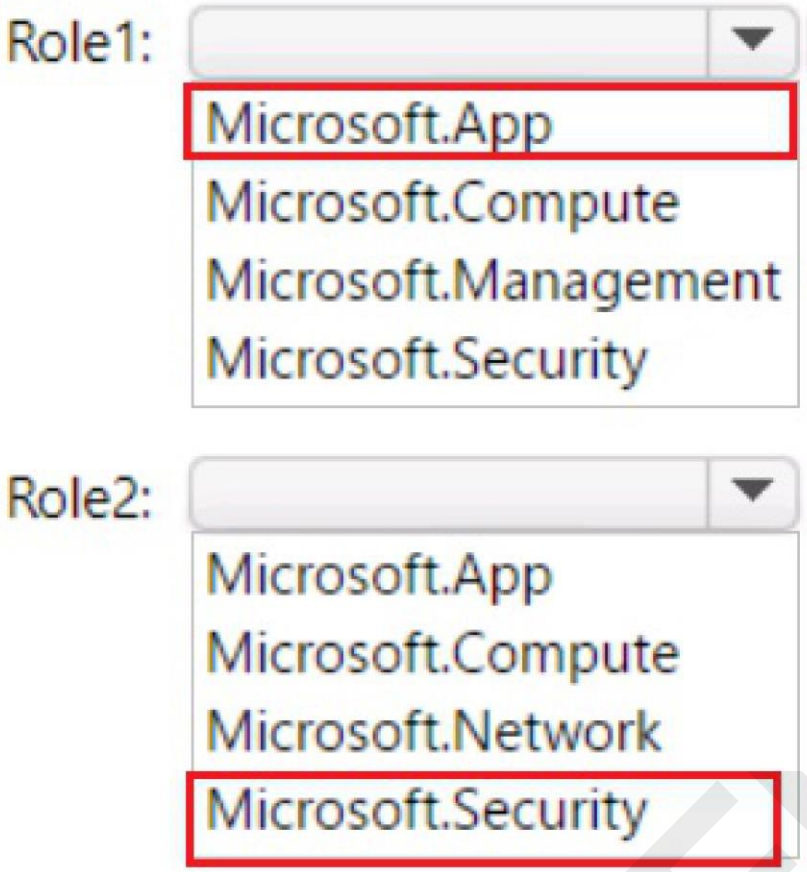
- Microsoft.App
- Microsoft.Compute
- Microsoft.Management
- Microsoft.Security

Role2:

- Microsoft.App
- Microsoft.Compute
- Microsoft.Network
- Microsoft.Security

Answer:

Answer Area



Explanation:

Role1: Microsoft.App.

Role2: Microsoft.Security.

Role1 requires permissions to create or delete instances of Azure Container Apps. The relevant resource provider for Azure Container Apps is Microsoft.App. This provider includes the necessary permissions to manage container app instances.

Role2 needs to enforce adaptive network hardening rules, which are part of Azure Security Center's capabilities. The Microsoft.Security resource provider contains the permissions required to enforce adaptive network hardening and other security-related configuration.

Question: 36 HOTSPOT

-

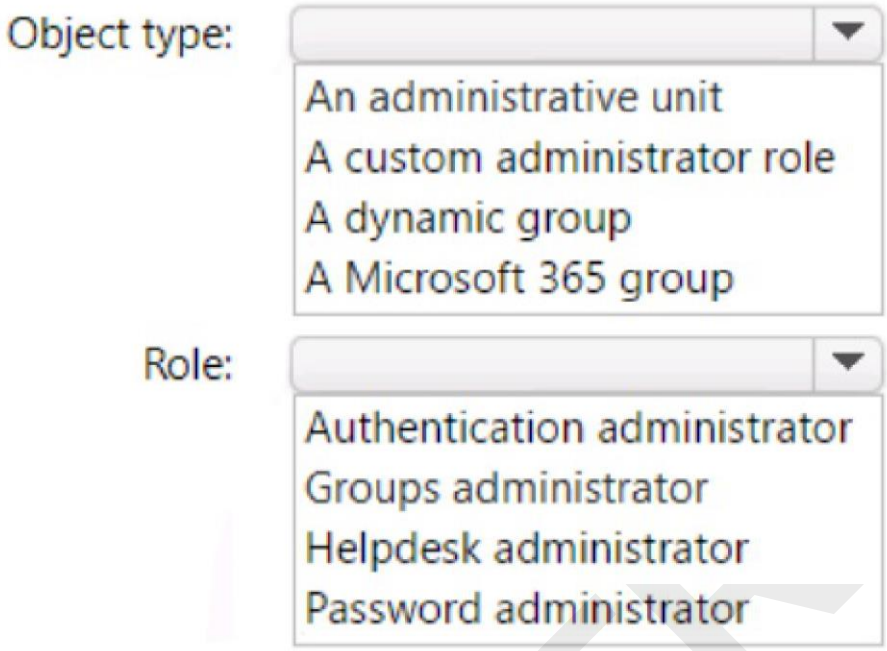
You have a Microsoft 365 tenant that has 5,000 users. One hundred of the users are executives. The executives have a dedicated support team.

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

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

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 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 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 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 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:

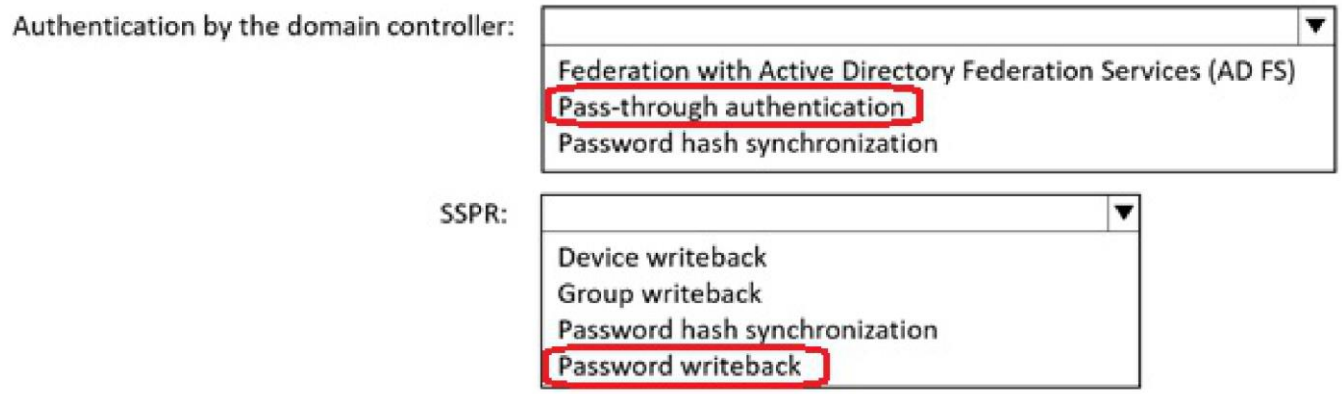
- Federation with Active Directory Federation Services (AD FS)
- Pass-through authentication
- Password hash synchronization

SSPR:

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

Answer:

Answer Area



Explanation:

pass- through auth

password write back

Question: 43

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

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 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:

A. Yes.

The Exchange Administrator role allows User1 to update the status of Identity Secure Score improvement actions. This role has the necessary permissions to make changes related to security recommendations.

Question: 46 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 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:

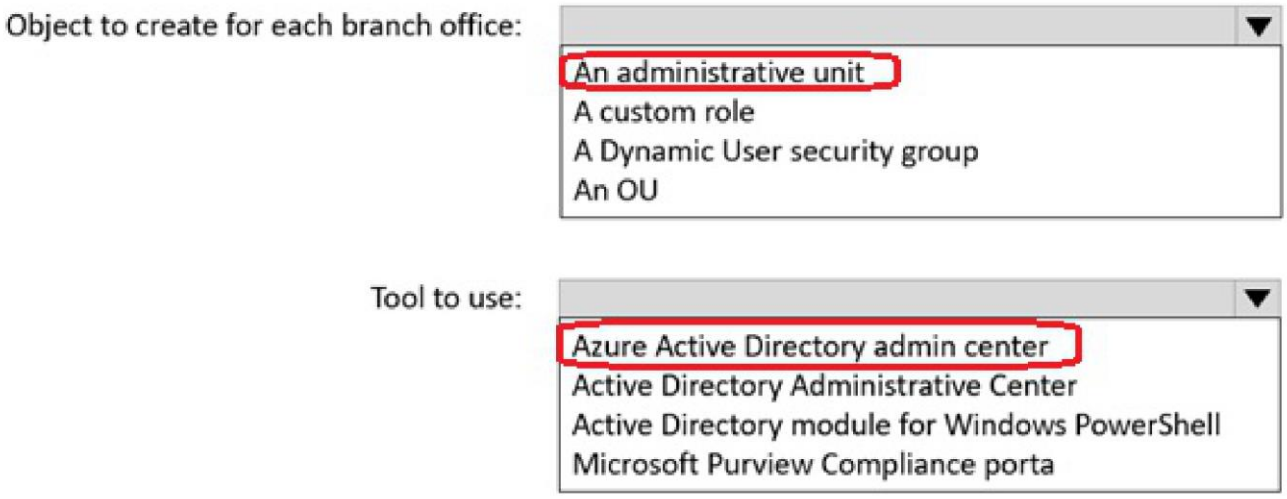
- An administrative unit
- A custom role
- A Dynamic User security group
- An OU

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 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

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

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

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: E

Explanation:

E. User1, Group1, VM1, and App1

In Azure Role-Based Access Control (RBAC), roles such as Contributor can be assigned to the following identity types:

Users (Azure AD users)

Groups (Azure AD security groups)

Service Principals (App registrations in Azure AD)

Managed Identities (System-assigned identities for VMs, applications, etc.)

Question: 52 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:

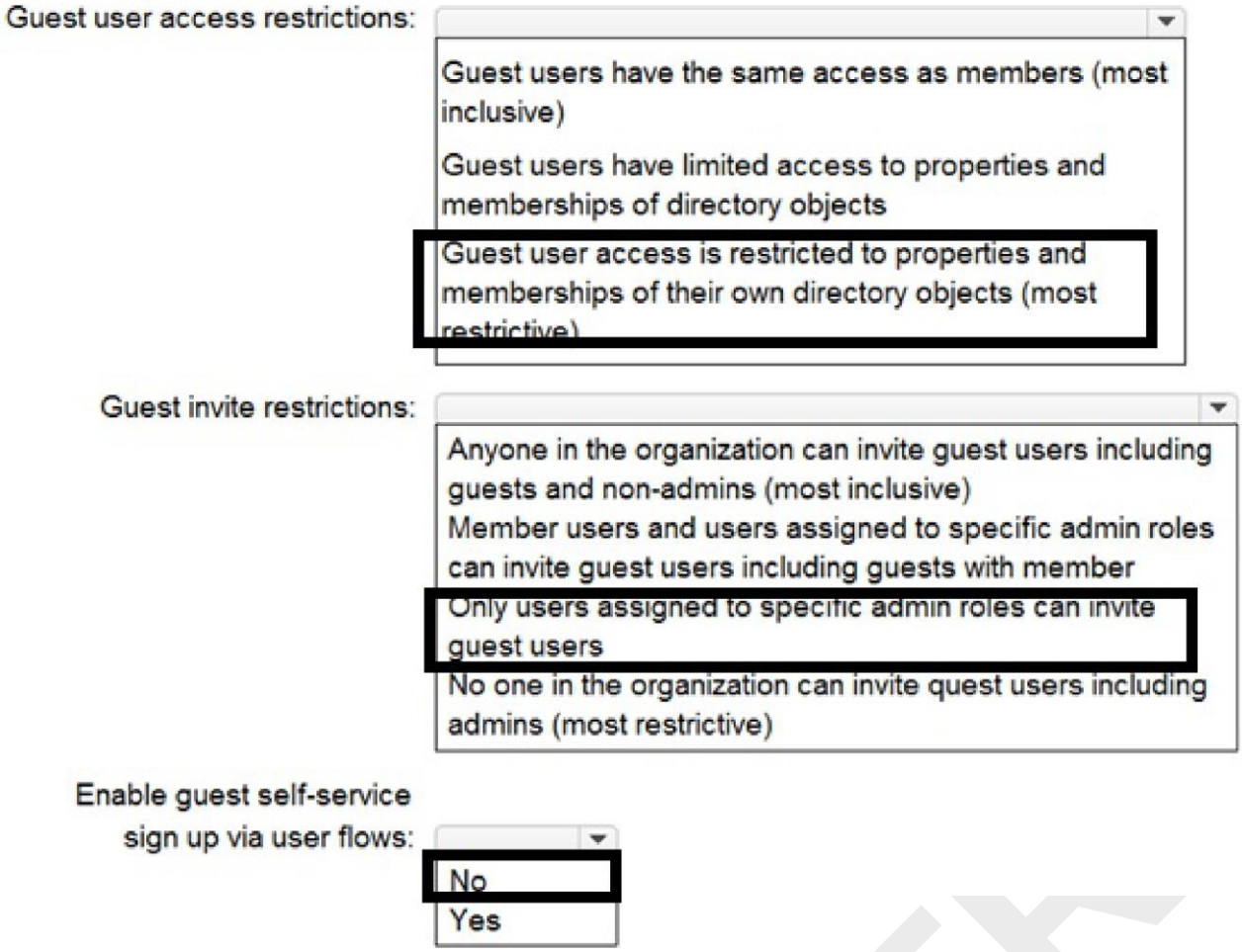
- Anyone in the organization can invite guest users including guests and non-admins (most inclusive)
- Member users and users assigned to specific admin roles can invite guest users including guests with member
- Only users assigned to specific admin roles can invite guest users
- No one in the organization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

Enable guest self-service sign up via user flows:

- No
- Yes

Answer:

Answer Area



Question: 53

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

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

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 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: D

Explanation:

D .Create a custom role and assign the role to Admin1.

A custom role allows you to specify highly granular permissions tailored to a user's unique requirements.

If you need Admin1 to have only the specified permissions with no additional tasks beyond the ones mentioned, a custom role can be meticulously designed to accomplish this.

For organizations with strict compliance needs or highly specific delegation requirements, creating custom roles might seem like a viable solution.

Question: 57 HOTSPOT -

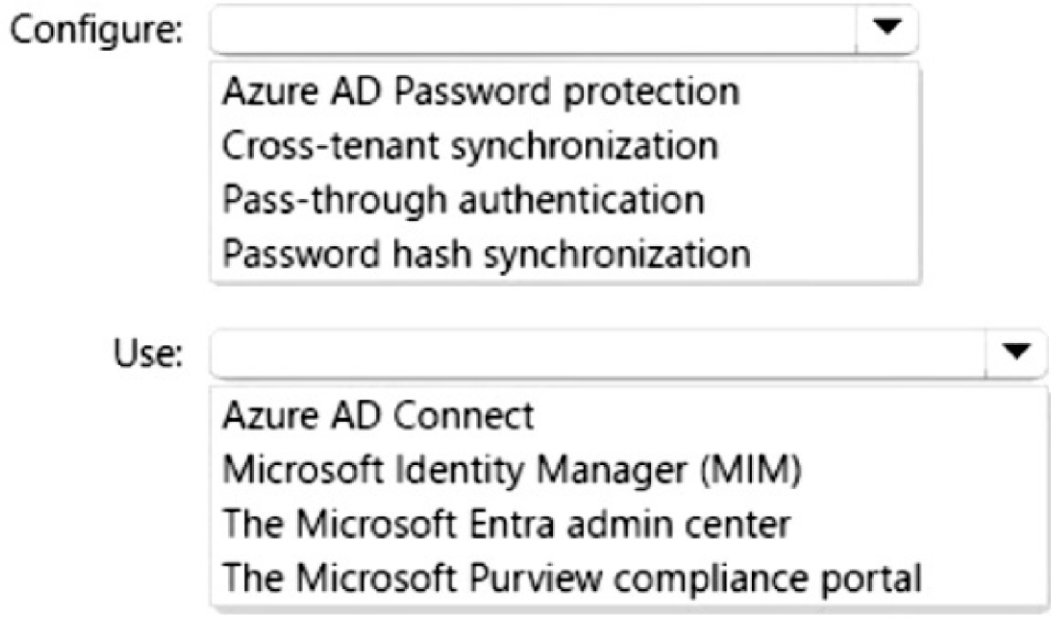
Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with an Azure AD tenant.

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.

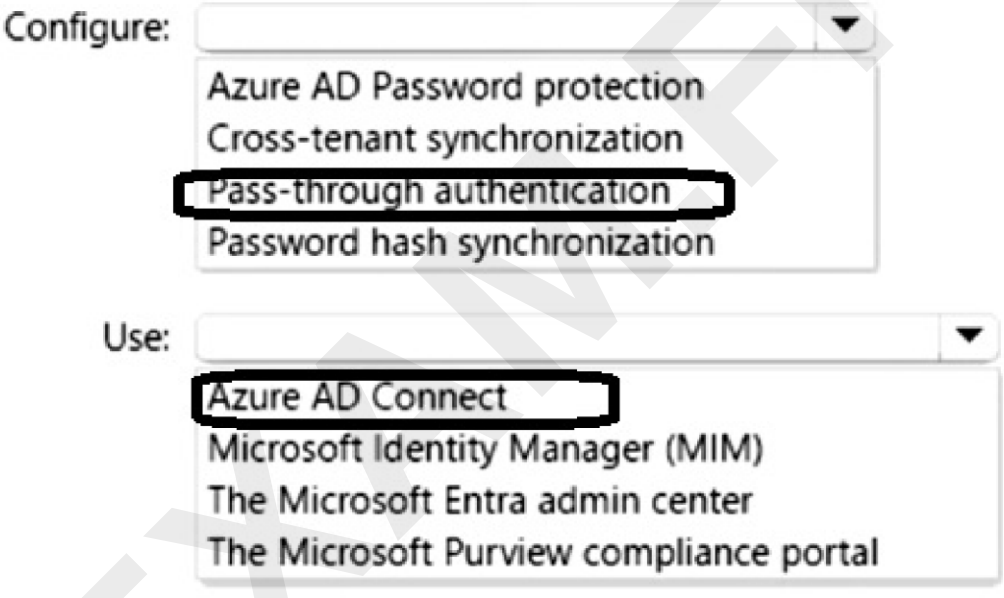
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area

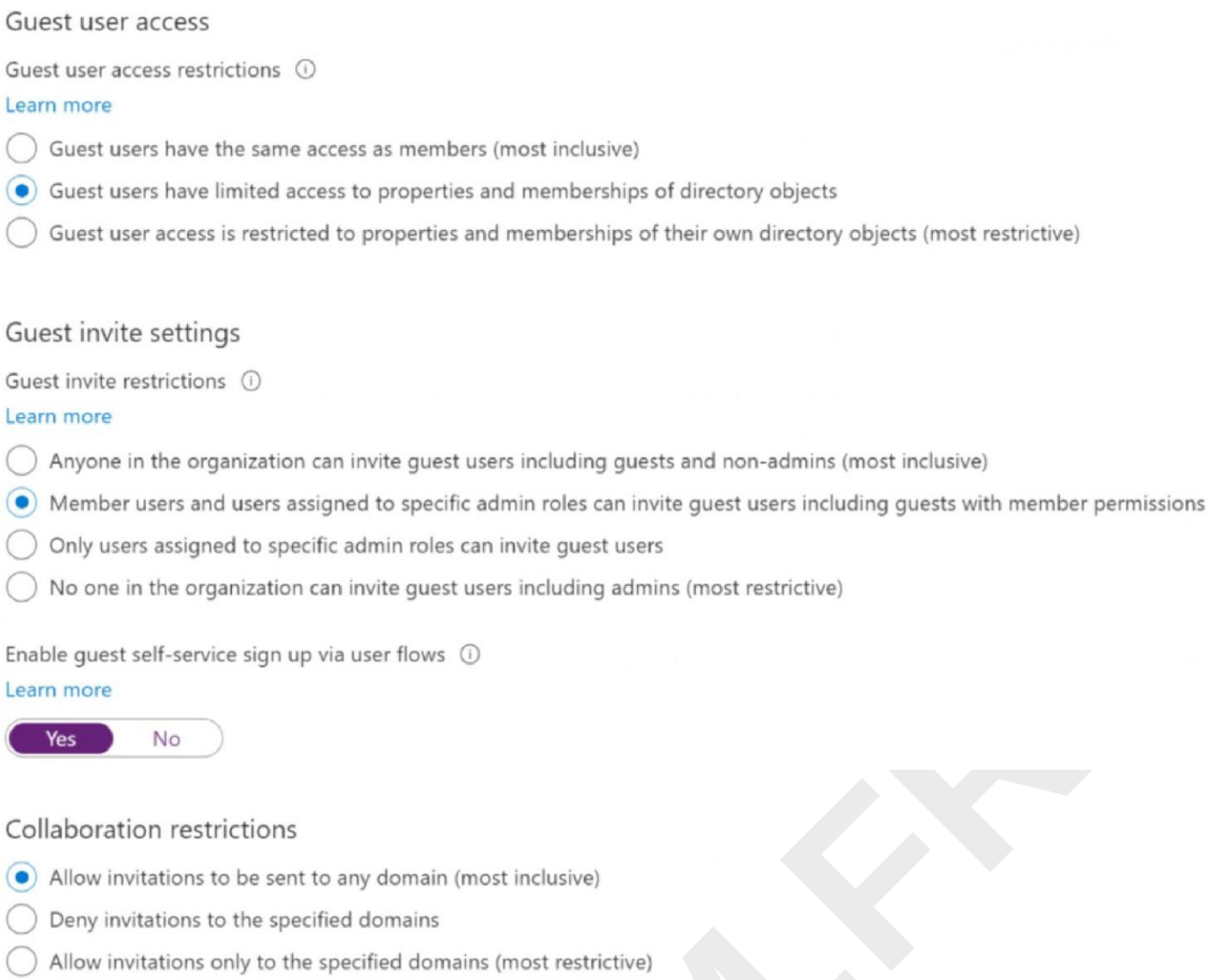


Explanation:

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

Question: 58

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

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.

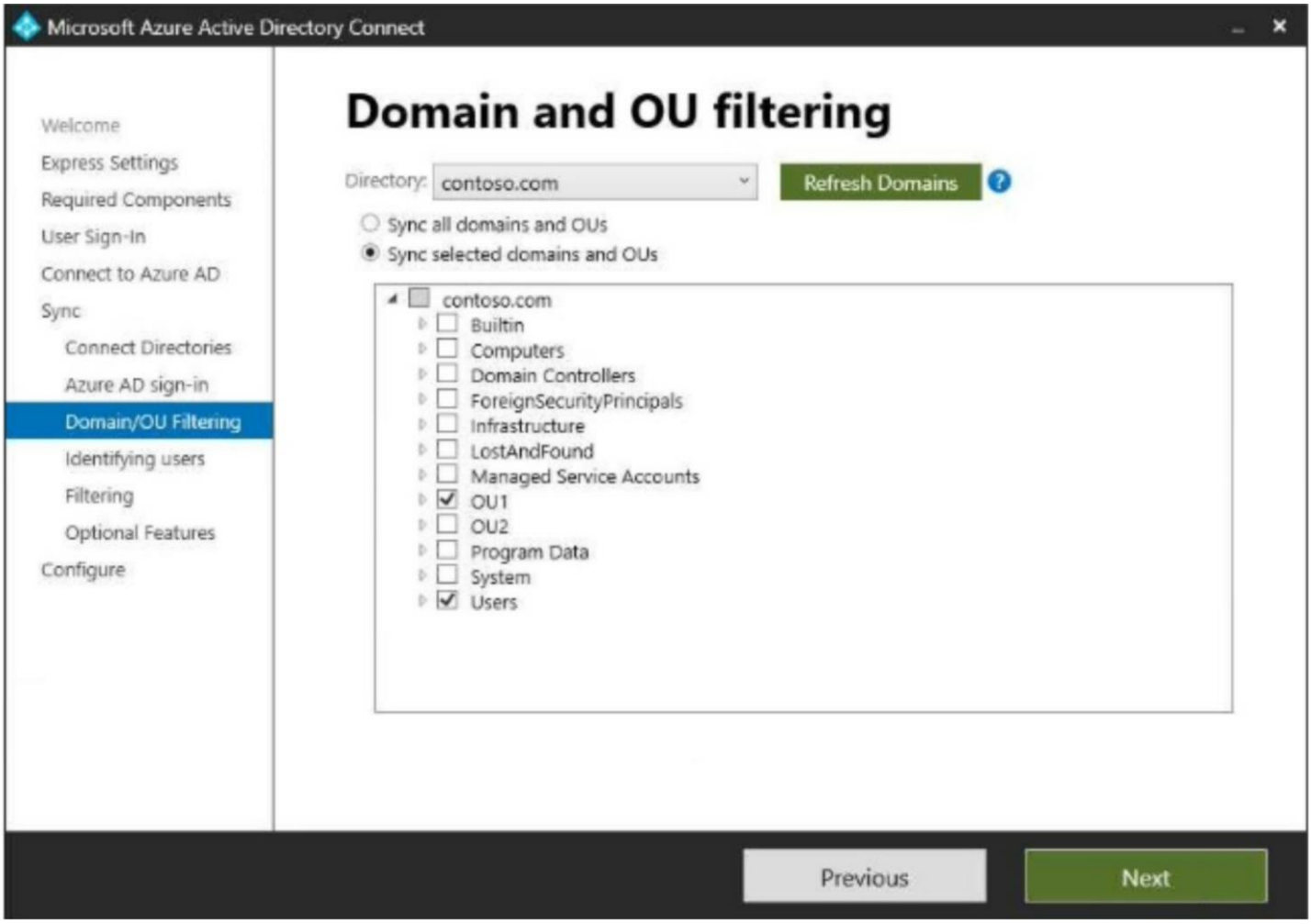
Question: 60

HOTSPOT
-

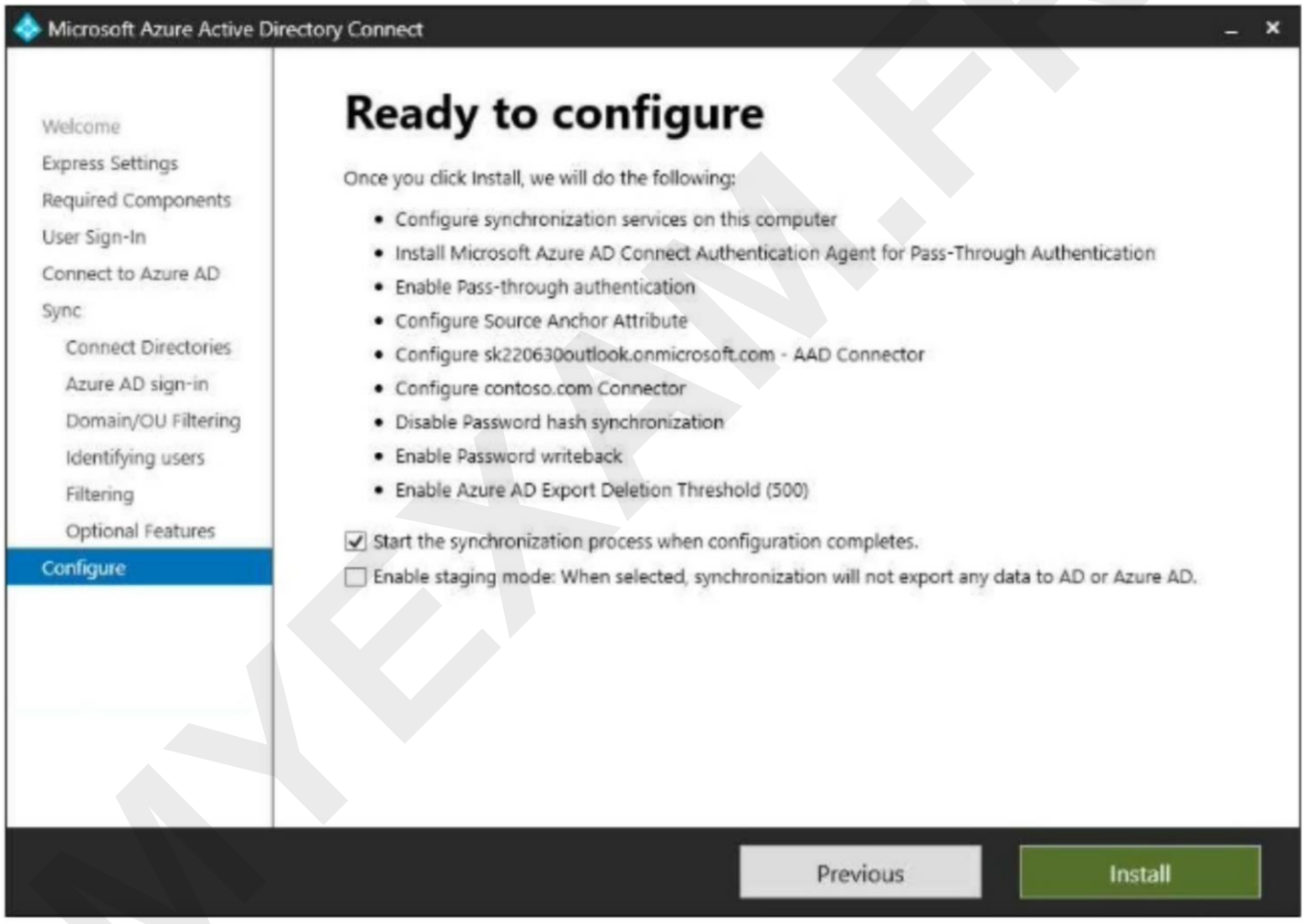
Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with Azure AD and contains the users shown in the following table.

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 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

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:

B. the Microsoft 365 admin center.

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

Question: 63

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: A

Explanation:

A. Update-MgOrganization.

To prevent users from creating accounts in the Azure AD tenant for self-service sign-up, you need to modify the organization's settings. The Update-MgOrganization cmdlet allows you to configure tenant-wide policies, including disabling self-service sign-up for users.

By using this cmdlet, you can set the appropriate parameters to block self-service sign-up, ensuring that users cannot create accounts in the tenant using their contoso.com email addresses.

Question: 64 HOTSPOT

-

You have an Azure AD tenant.

You need to configure the following External Identities features:

•B2B collaboration

•Monthly active users (MAU)-based pricing

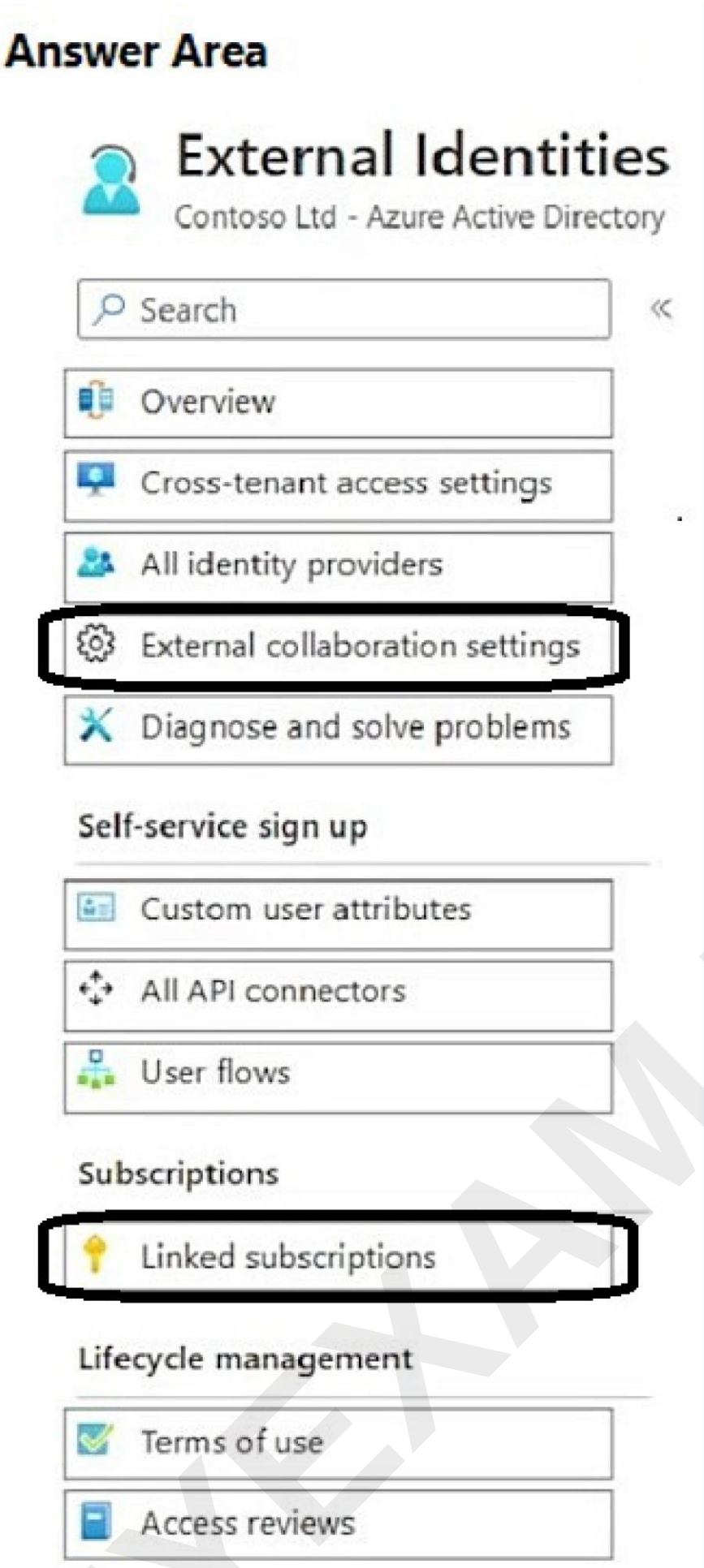
Which two settings should you configure? To answer, select the settings in the answer area. NOTE:

Each correct selection is worth one point.

Answer Area

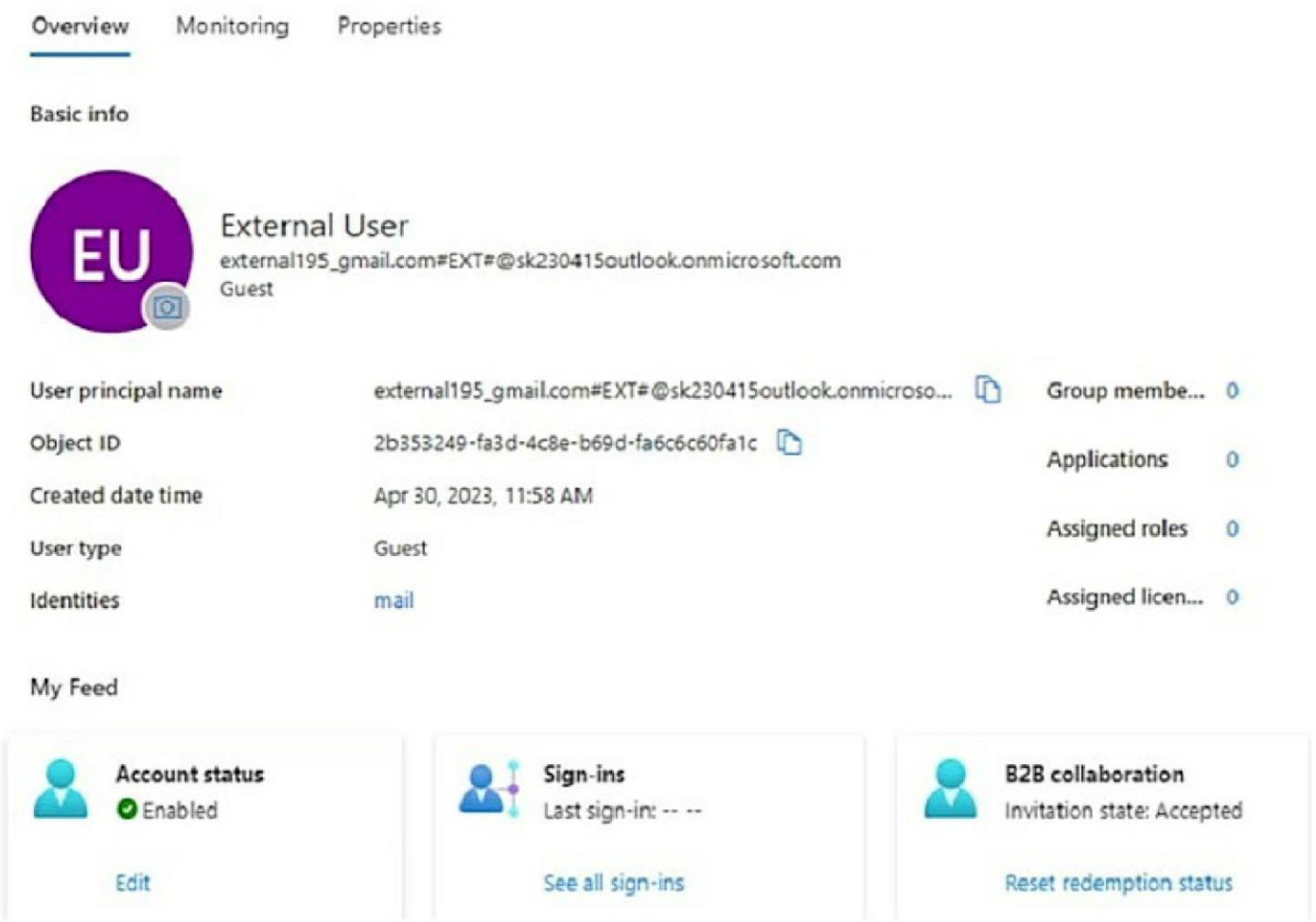
Answer:

Answer Area



Question: 65

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

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

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.

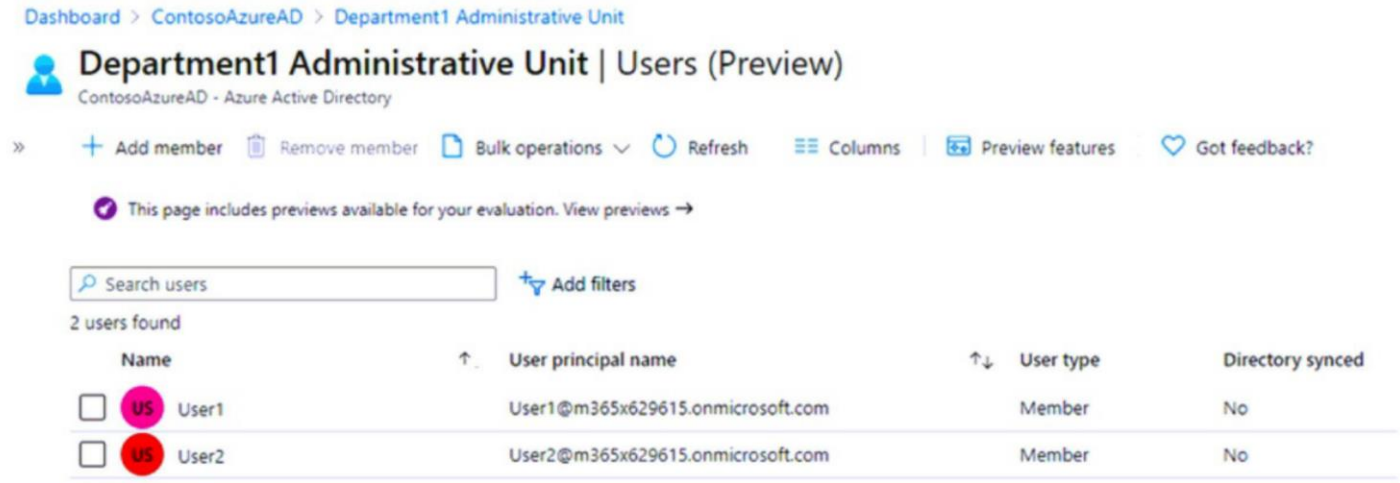
Question: 68

HOTSPOT

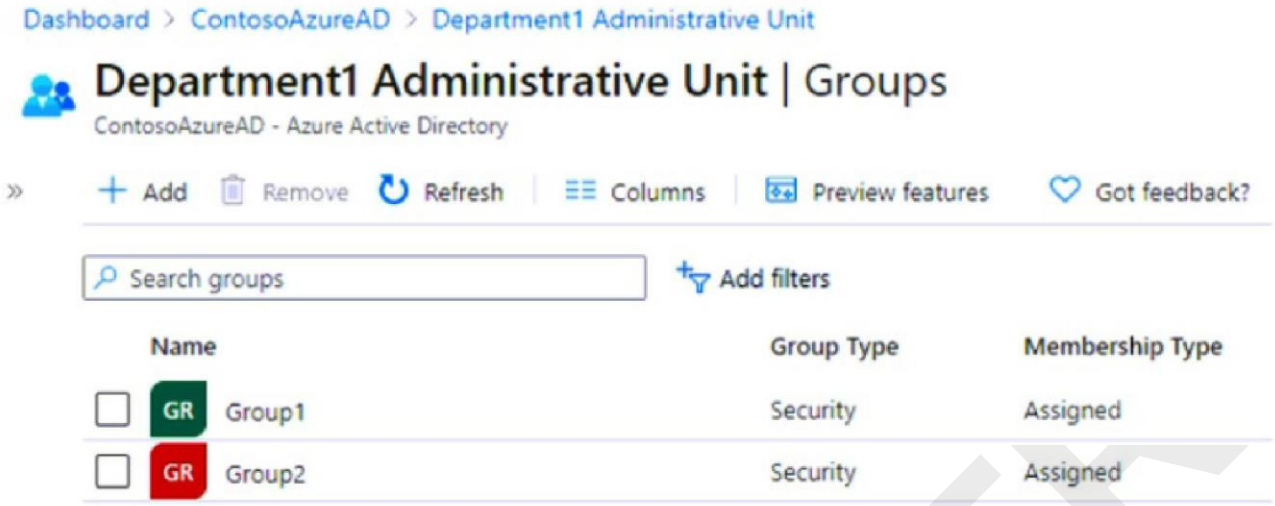
-

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

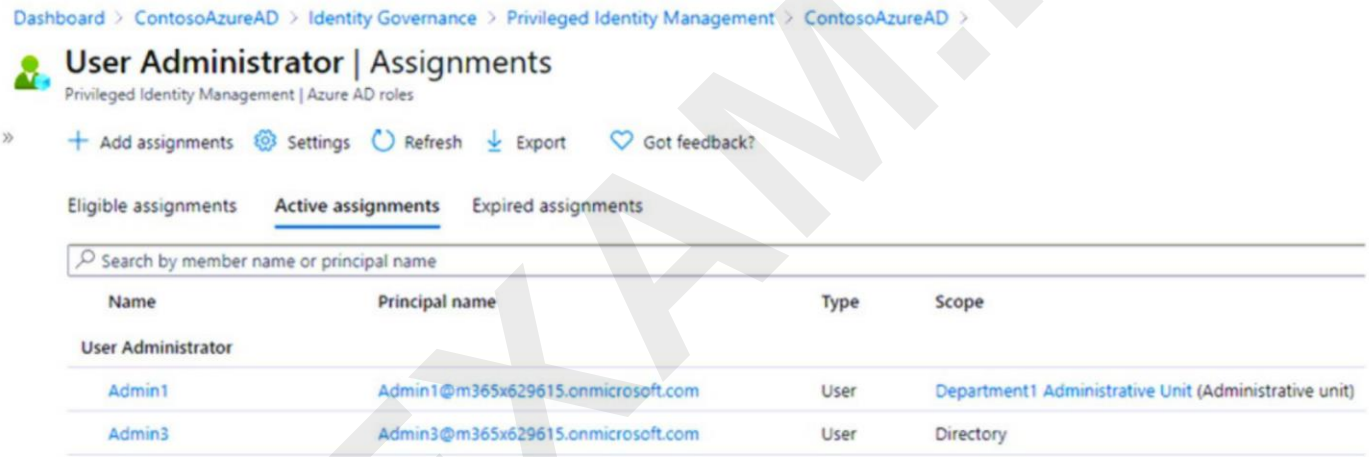
Department1 has the users shown in the Users exhibit. (Click the Users tab.)



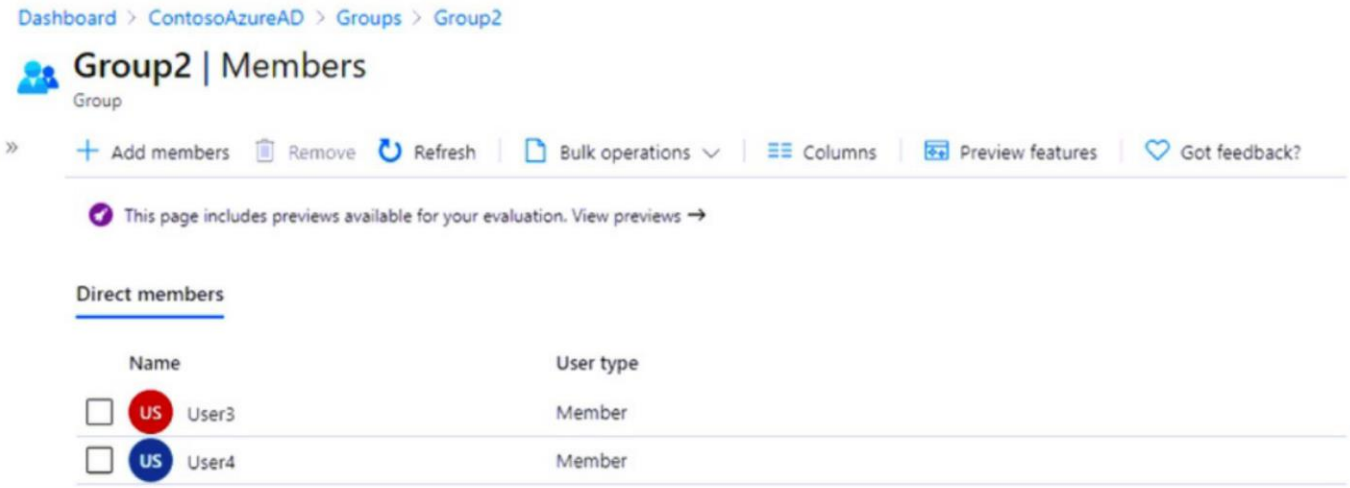
Department1 has the groups shown in the Groups exhibit. (Click the Groups tab.)



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

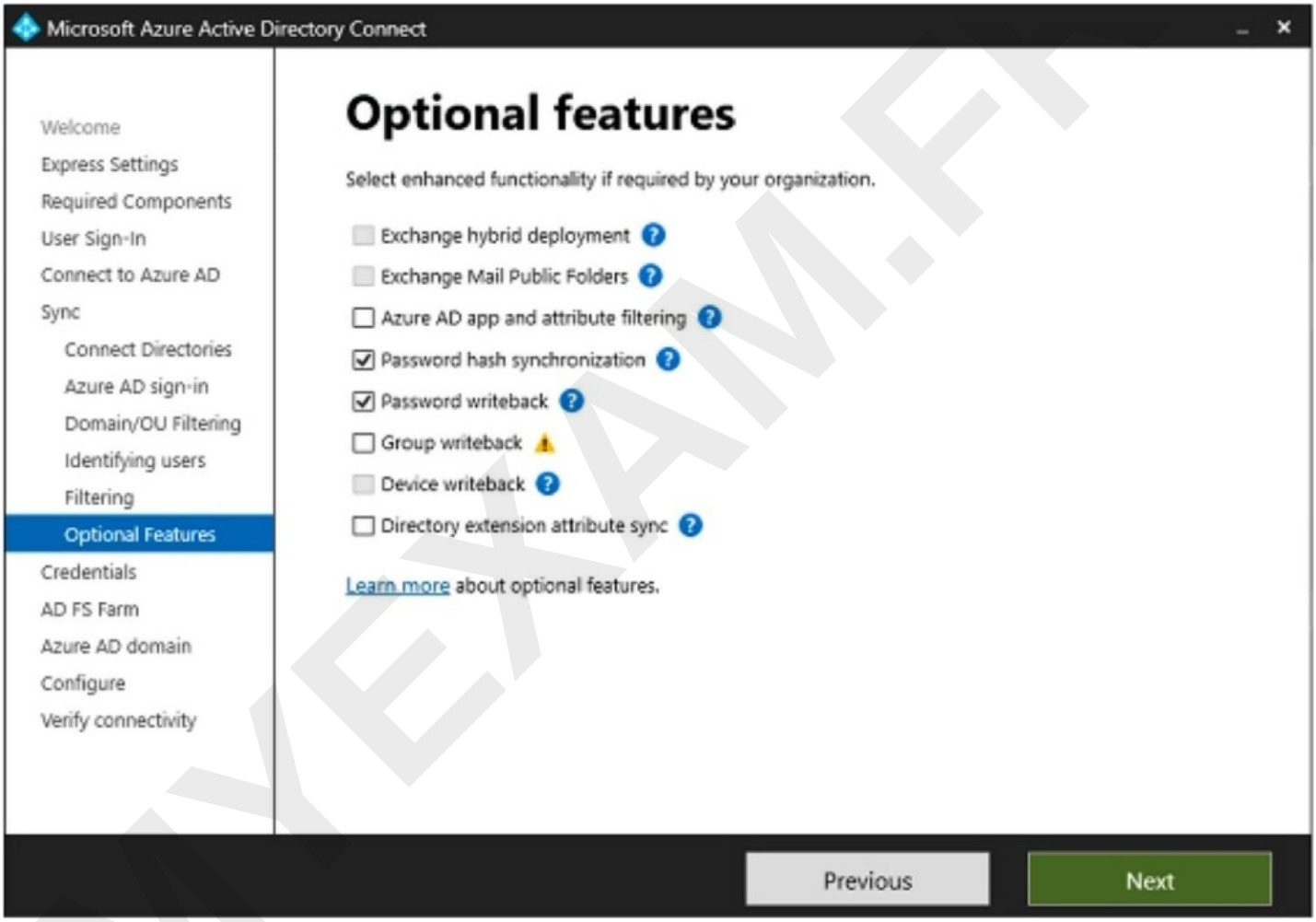
HOTSPOT
-

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

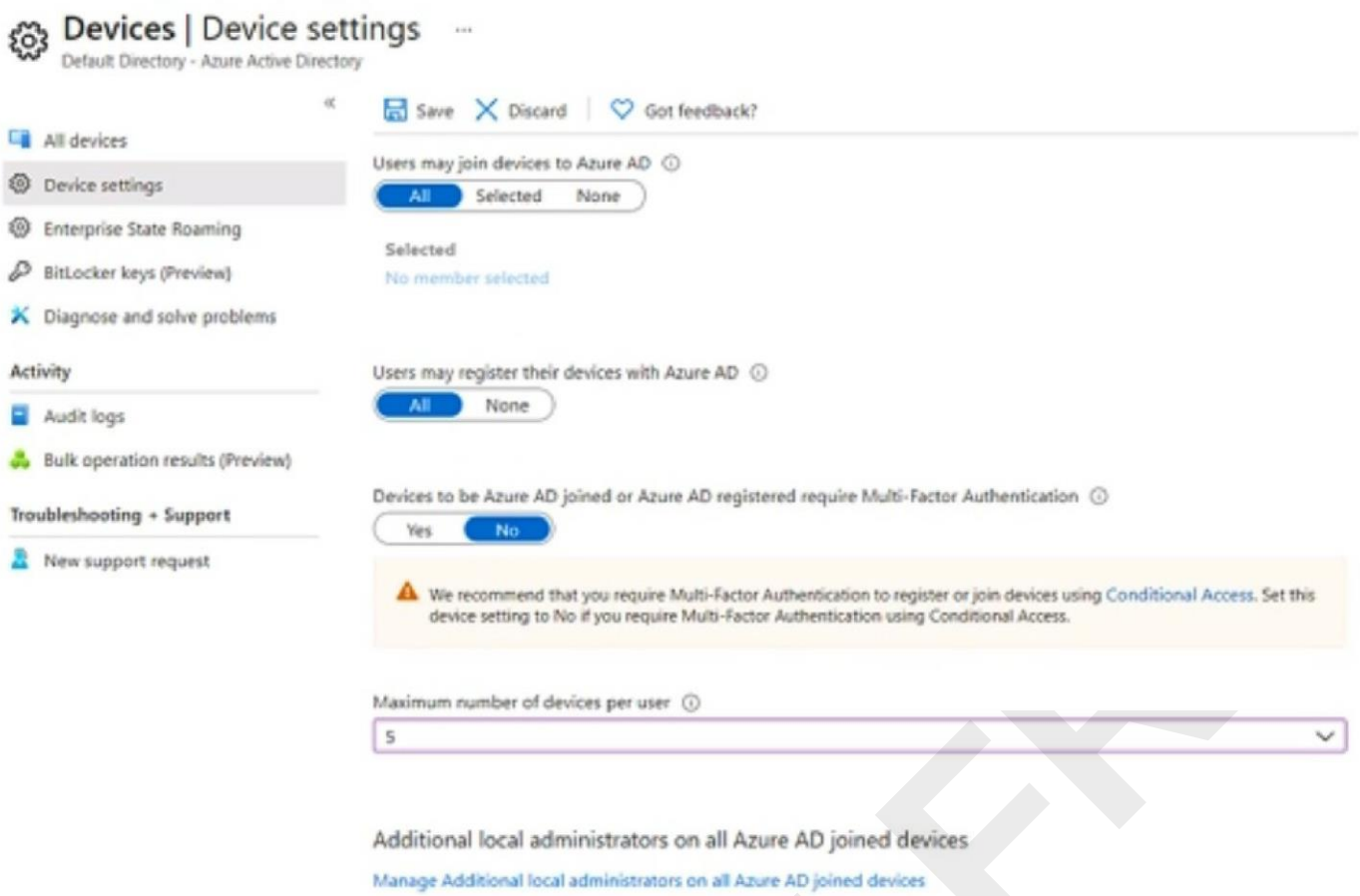
Question: 70

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 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 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: C

Explanation:
Minimum Number of Role Assignments:
To meet these requirements, User1 needs a combination of Reader, Virtual Machine Contributor, and Storage Account Contributor roles. Since there is overlap in the roles that allow User1 to restart VMs and create VMs, we can optimize the number of role assignments.

Reader role at the subscription level.

Virtual Machine Contributor role at RG1 (to allow both VM creation and VM restart in RG1).

Storage Account Contributor role at RG1.

Conclusion:
The minimum number of role assignments required is 3.

the correct answer is: C. 3

Question: 73 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

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

DRAG DROP
-

Your network contains an on-premises Active Directory domain named contoso.com that syncs with Microsoft Entra ID by using Microsoft Entra Connect. The domain contains the users shown in the following table.

Name	User principal name (UPN)	Proxy address
User1	user1@contoso.com	smtp: user1@contoso.com smtp: sales@contoso.com
User2	user2@contoso.com	smtp: user2@contoso.com smtp: user.2@contoso.com smtp: service@contoso.com

From Active Directory Users and Computers, you add the following user:

•Name: User3
•UPN:
•Proxy addresses: smtp: , smtp:

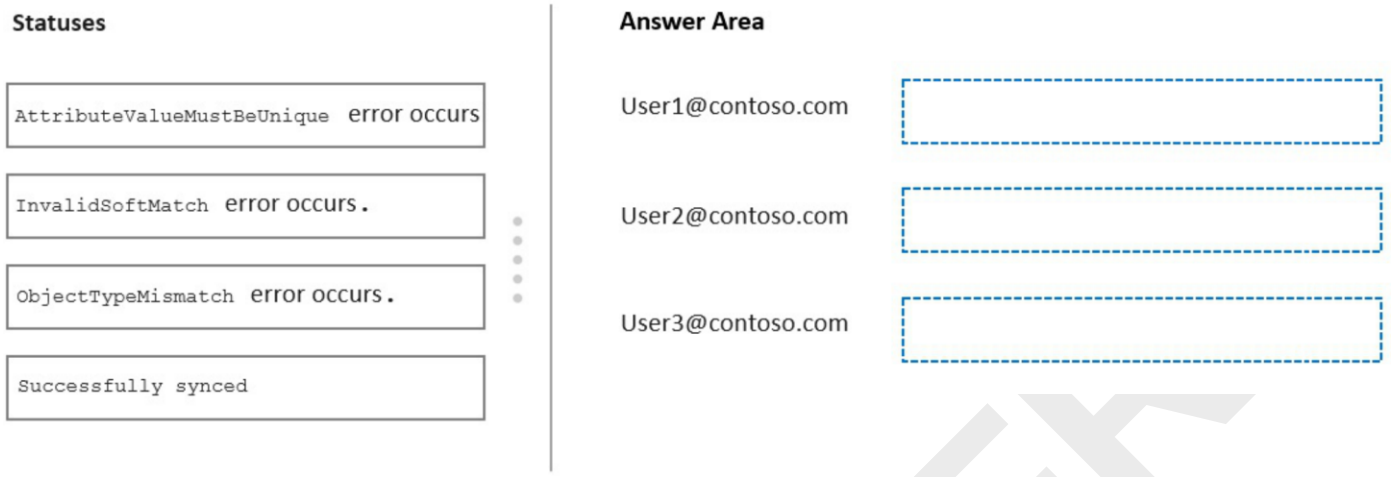
From Active Directory Users and Computers, you update the proxyAddresses attribute for each user as shown in the following table.

Name	Proxy address
User1	smtp: admin@contoso.com
User2	smtp: sales@contoso.com

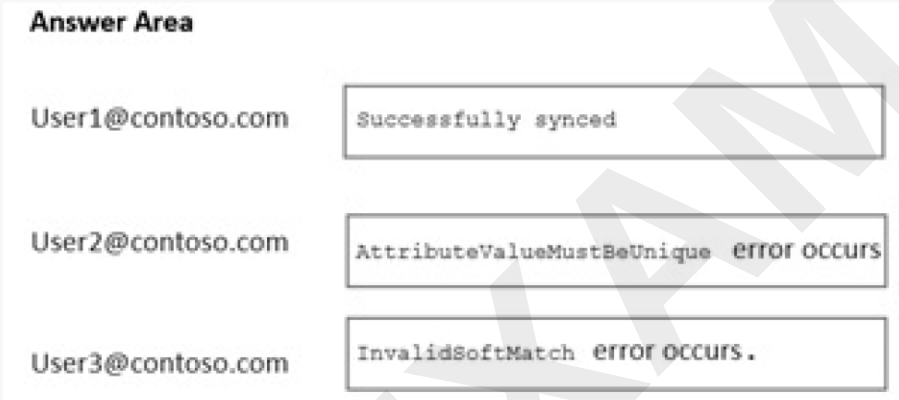
You trigger a manual synchronization.

Which sync status will Microsoft Entra Connect sync return for each user? To answer, drag the appropriate status to the correct users. Each status may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



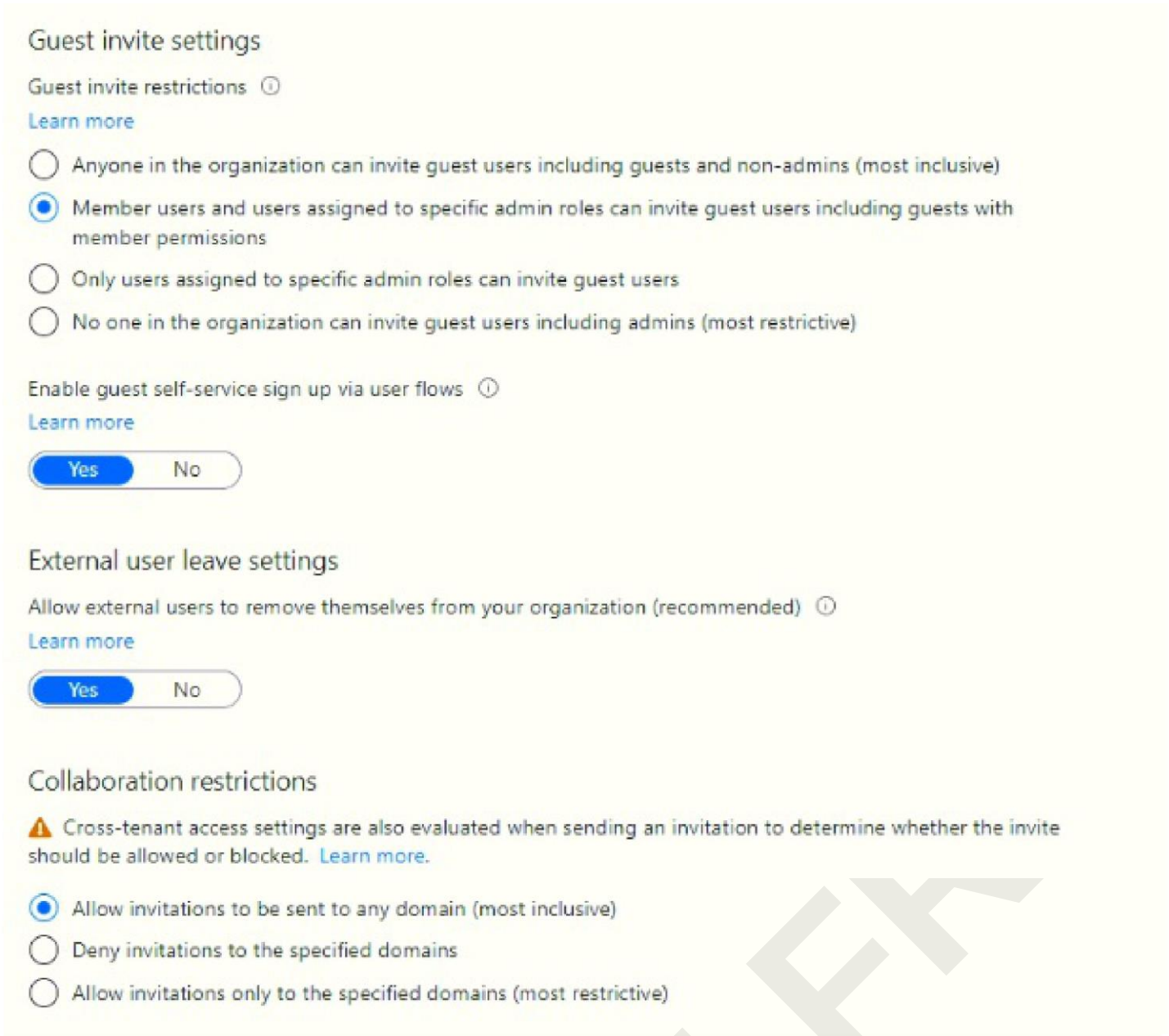
Answer:



Question: 76

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: 77

You have an Azure subscription named Sub1 that contains a virtual machine named VM1.

You need to enable Microsoft Entra login for VM1 and configure VM1 to access the resources in Sub1.

Which type of identity should you assign to VM1?

A.Microsoft Entra user account
B.user-assigned managed identity
C.Azure Automation account
D.system-assigned managed identity

Answer: D

Explanation:

System-assigned managed identity: This type of managed identity is enabled directly on an Azure resource. In this case, enabling a system-assigned managed identity on VM1 would allow VM1 to authenticate with other Azure resources within Sub1, using the identity associated with VM1.

Question: 78

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: 79

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: 80

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

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

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

What should you use?

A.the Identity Governance blade in the Microsoft Entra admin center
B.the Update-MgGroup cmdlet
C.the Set-MgUserLicense cmdlet
D.the Administrative units blade in the Microsoft Entra admin center

Answer: C

Explanation:

The Set-MgUserLicense cmdlet (part of Microsoft Graph PowerShell) allows you to add or remove licenses for a user programmatically.

You can automate the removal of the E3 license from all 2,500 users by scripting the process.

This approach avoids manual removal and provides the least administrative effort compared to doing it through the GUI.