Topic 1 - Question Set 1

Question #1 *Topic 1*

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

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

The groups are configured as shown in the following table.

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

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

A. Group1 and Group4 only

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

C. Group1 and Group2 only

D. Group1 only

E. Group1, Group2, Group4, and Group5 only

Correct Answer: *C*

Reference:

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

Community vote distribution

B (43%) E (29%) C (28%)

Question #2 *Topic 1*

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

A. Set-MsolCompanySettings

B. Set-MsolDomainFederationSettings

C. Update-MsolfederatedDomain

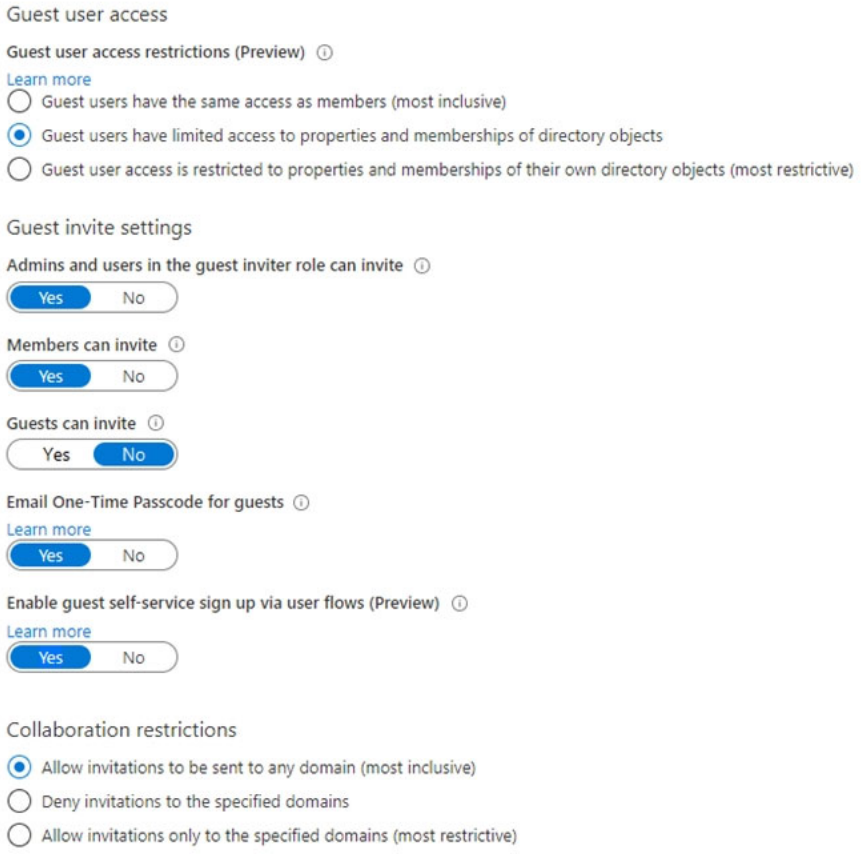
D. Set-MsolDomain

Correct Answer: *A*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/directory-self-service-signup

Community vote distribution

A (100%)

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

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

Which users will be emailed a passcode?

A. User2 only

B. User1 only

C. User1 and User2 only

D. User1, User2, and User3

Correct Answer: *A*

Reference:

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

Community vote distribution

A (46%) C (31%) B (23%)

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

A. the Identity Governance blade in the Azure Active Directory admin center

B. the Set-AzureAdUser cmdlet

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

D. the Set-WindowsProductKey cmdlet

Correct Answer: *C*
You can unassign licenses from users on either the Active users page, or on the Licenses page. The method you use depends on whether you want to unassign product licenses from specific users or unassign users licenses from a specific product.
Note:
There are several versions of this question in the exam. The question has two possible correct answers:
1. the Licenses blade in the Azure Active Directory admin center
2. the Set-MsolUserLicense cmdlet
Other incorrect answer options you may see on the exam include the following:
- the Administrative units blade in the Azure Active Directory admin center
- the Groups blade in the Azure Active Directory admin center
- the Set-AzureAdGroup cmdlet
Reference:
https://docs.microsoft.com/en-us/microsoft-365/admin/manage/remove-licenses-from-users?view=o365-worldwide

Community vote distribution

C (100%)

HOTSPOT -

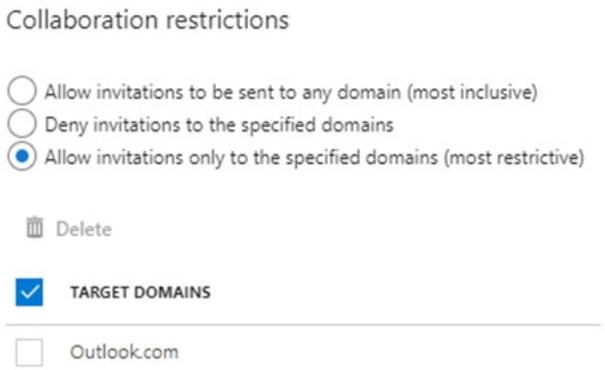
You have a Microsoft 365 tenant named contoso.com.

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 user3@adatum.com to the site.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

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

Answer Area

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

Box 1: Yes -

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

Box 2. Yes -

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

Box 3. No -
Invitations can only be sent to outlook.com. Therefore, User3 will not receive an invitation.

Question #6 *Topic 1*

You have an Azure Active Directory (Azure AD) tenant named contoso.com.
You plan to bulk invite Azure AD business-to-business (B2B) collaboration users.
Which two parameters must you include when you create the bulk invite? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. email address

B. redirection URL

C. username

D. shared key

E. password

Correct Answer: *AB*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/tutorial-bulk-invite

Community vote distribution
AB (100%)

Question #7 *Topic 1*

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

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

Which objects can you add as members to Group3?

A. User2 and Group2 only

B. User2, Group1, and Group2 only

C. User1, User2, Group1 and Group2

D. User1 and User2 only

E. User2 only

Correct Answer: *E*
Reference:
https://bitsizedbytes.wordpress.com/2018/12/10/distribution-security-and-office-365-groups-nesting/

Community vote distribution
E (67%) D (33%)

DRAG DROP -

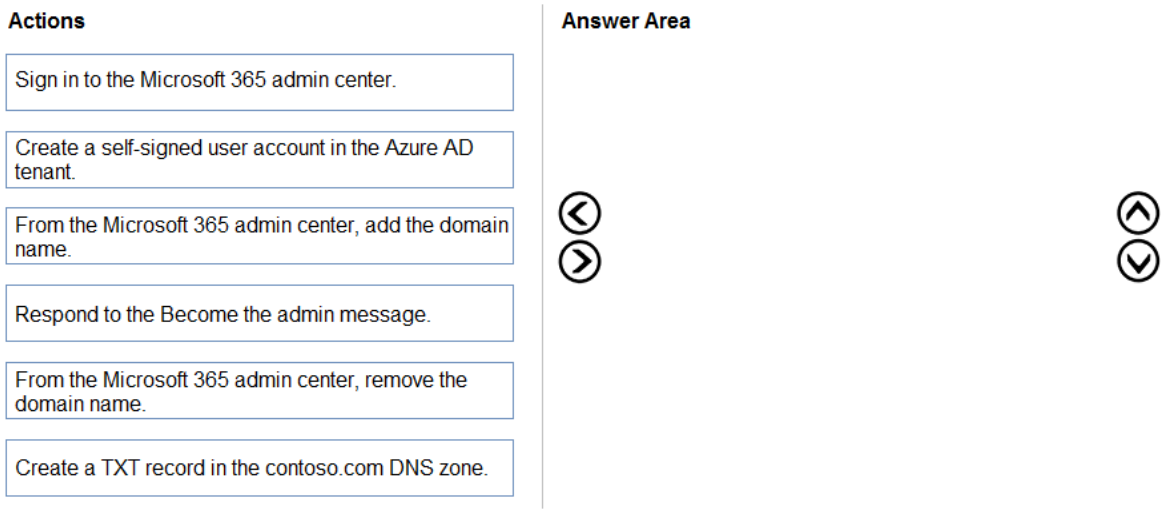
You have an on-premises Microsoft Exchange organization that uses an SMTP address space of contoso.com.

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

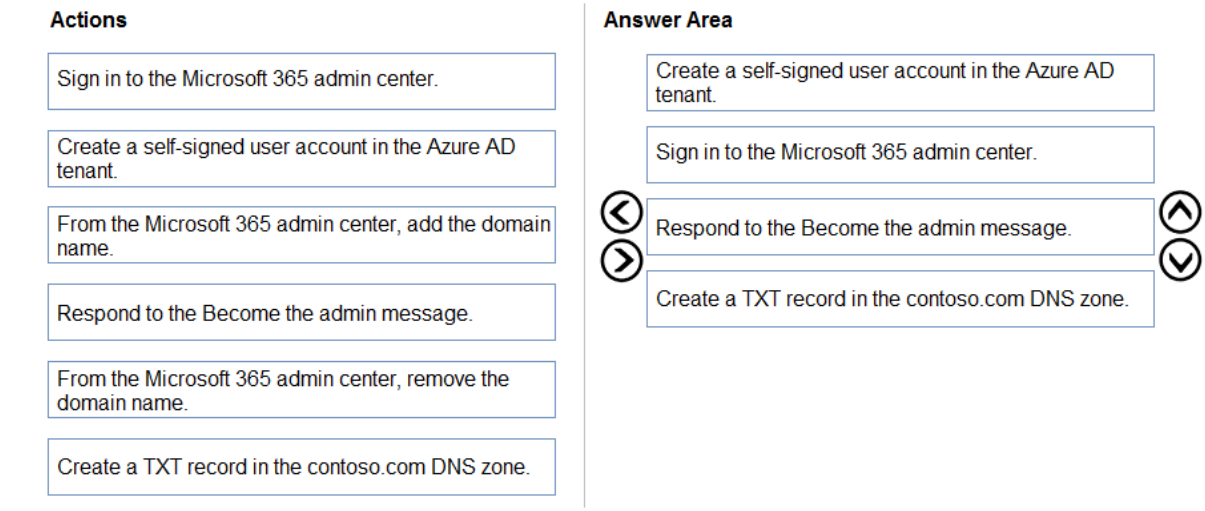
You need to gain global administrator privileges to the Azure Active Directory (Azure AD) tenant that contains the self-signed users.

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:



Correct Answer:



Reference:

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

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

Correct Answer:

Answer Area

GroupA:
- User1 only
- User1 and Group1 only
- User1, Group1, and Group2 only
- User1, Group1, and Group4 only
- **User1, Group1, Group2, and Group3 only**
- User1, Group1, Group2, Group3, and Group4

GroupB:
- **User1 only**
- User1 and Group4 only
- User1, Group1, and Group4 only
- User1, Group1, Group2, and Group4 only
- User1, Group1, Group2, Group3, and Group4

Reference:

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

Question #10 *Topic 1*

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

A. Yes

B. No

Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn

Community vote distribution

B (100%)

Question #11 *Topic 1*

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

A. Yes

B. No

Correct Answer: *A*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn

Community vote distribution

A (100%)

Question #12 *Topic 1*

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

A. Yes

B. No

Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn

Community vote distribution
B (100%)

Question #13 *Topic 1*

You have an Azure Active Directory (Azure AD) tenant that contains the following objects.
- A device named Device1
- Users named User1, User2, User3, User4, and User5
- Five groups named Group1, Group2, Group3, Group4, and Group5

The groups are configured as shown in the following table.

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

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

A. 0

B. 2

C. 3

D. 4

Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-group-advanced

Community vote distribution
B (100%)

Question #14 *Topic 1*

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

A. Run the New-AzADUser cmdlet.

B. Configure the External collaboration settings.

C. Add a WS-Fed identity provider.

D. Create a guest user account in contoso.com.

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

Community vote distribution

D (100%)

Question #15 *Topic 1*

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

A. Create an inbound synchronization rule for the Windows Azure Active Directory connector.

B. Configure a Full Import run profile.

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

D. Configure an Export run profile.

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

Community vote distribution

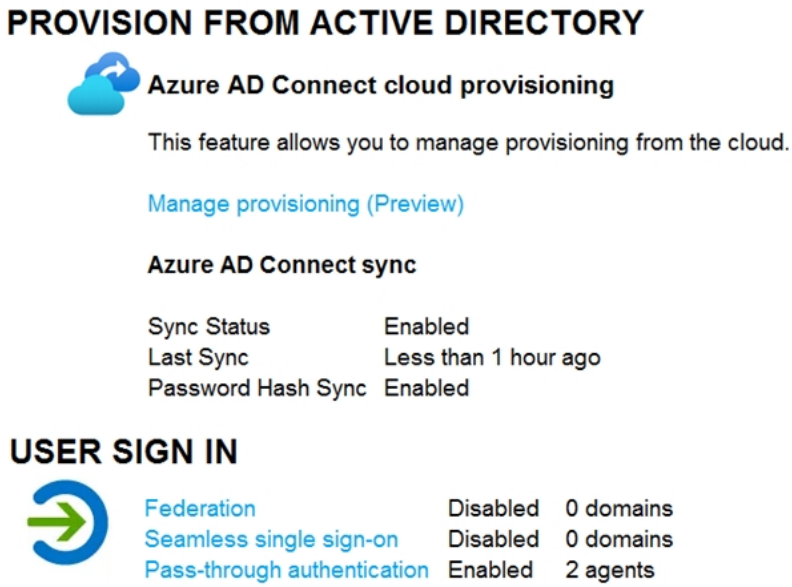
C (100%)

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

Correct Answer: *A*

Reference:

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

Community vote distribution

A (100%)

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

A. Yes

B. No

Correct Answer: *B*

Community vote distribution

B (100%)

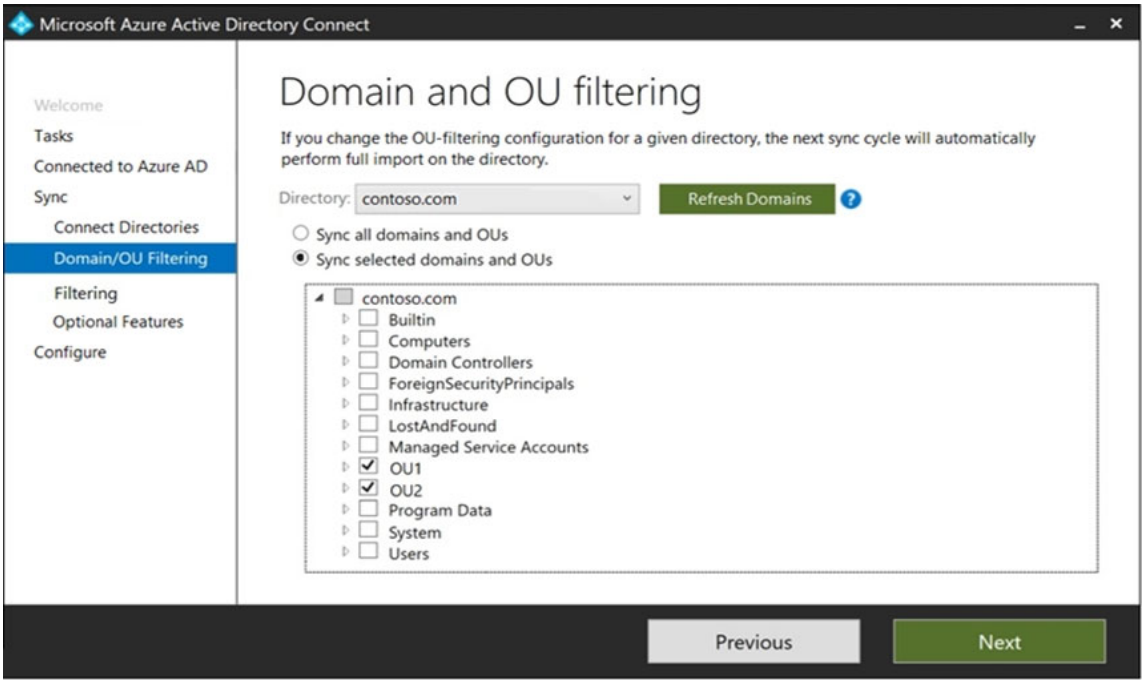
HOTSPOT -

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

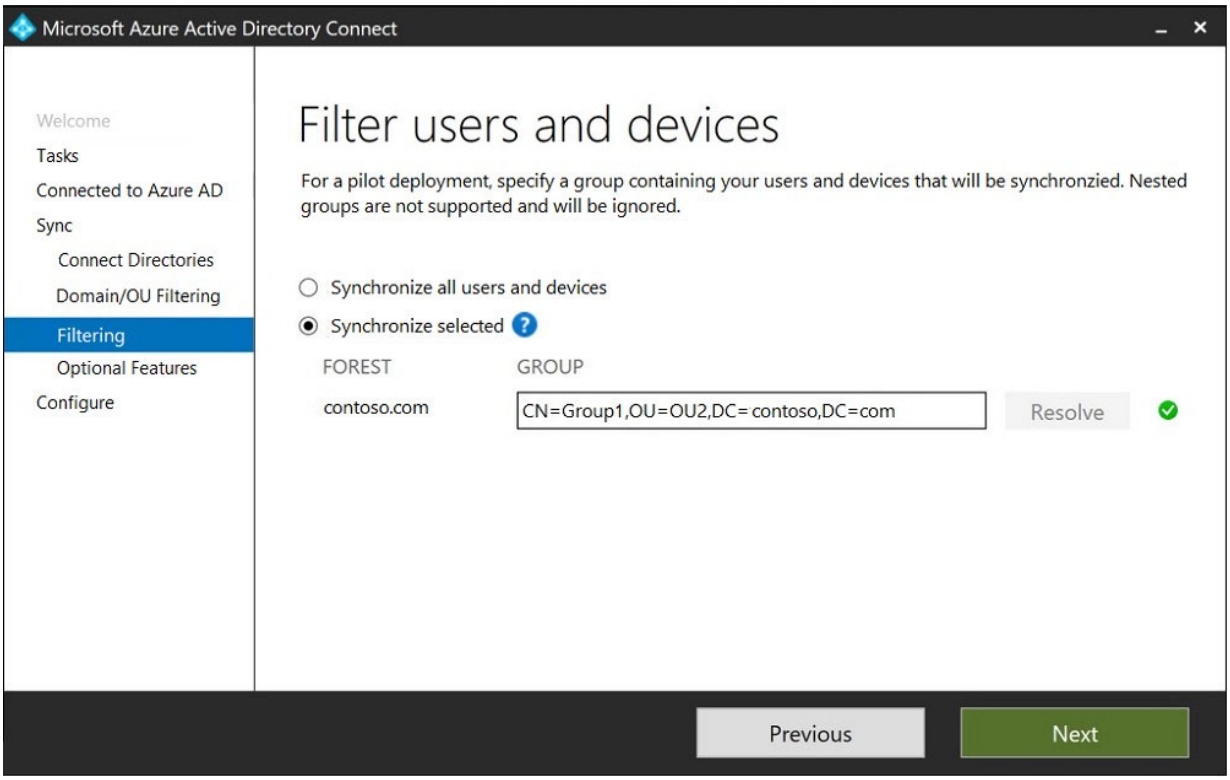
Name	Type	In organizational unit (OU)	Description
User1	User	OU1	User1 is a member of Group1.
User2	User	OU1	User2 is not a member of any groups.
Group1	Security group	OU2	User1 and Group2 are members of Group1.
Group2	Security group	OU1	Group2 is a member of Group1.

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.	○	○

Correct Answer:

Answer Area

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

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

Reference:

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

Question #19 *Topic 1*

You have an Azure Active Directory (Azure AD) tenant named contoso.com.
You need to ensure that Azure AD External Identities pricing is based on monthly active users (MAU).
What should you configure?

A. a user flow

B. the terms of use

C. a linked subscription

D. an access review

Correct Answer: *C*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/external-identities-pricing

Community vote distribution

C (100%)

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.	

Correct 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.

Reference:

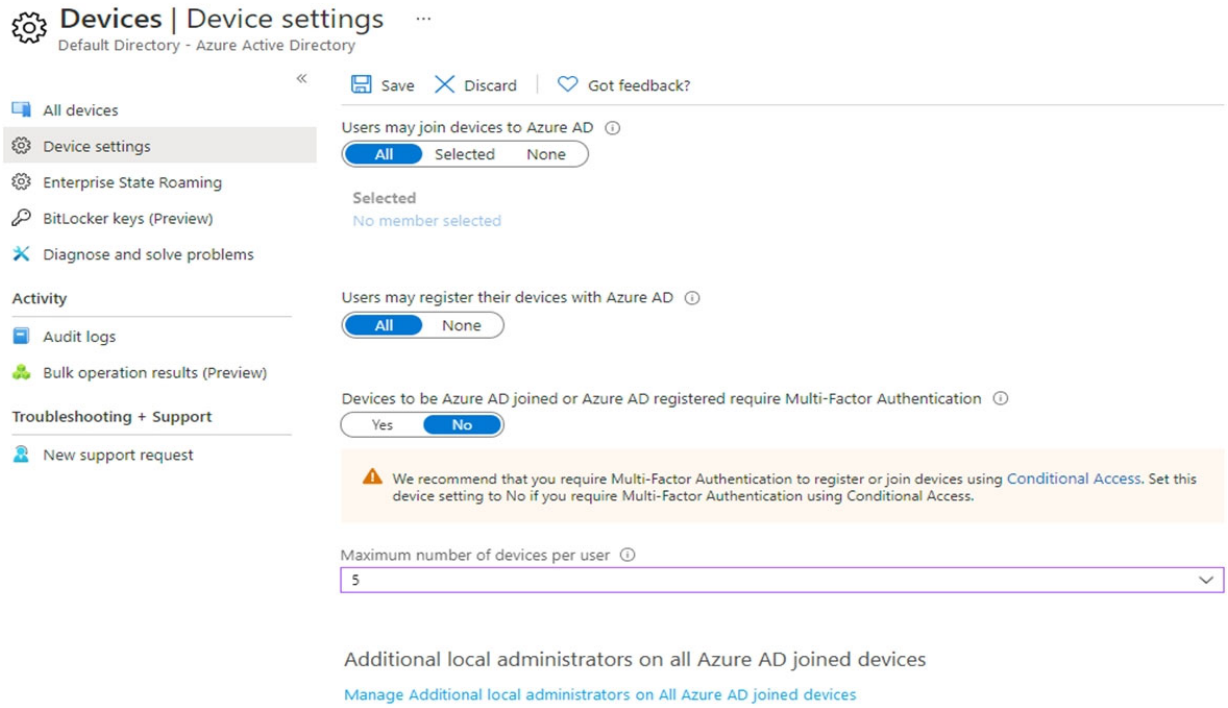
https://practical365.com/configure-a-custom-domain-in-office-365/

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.	○	○

Correct Answer:

Answer Area

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

Box 1: Yes -

Users may join 5 devices to Azure AD.

Box 2: No -

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

Box 3: No -

An additional local device administrator has not been applied

Reference:

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

DRAG DROP -

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

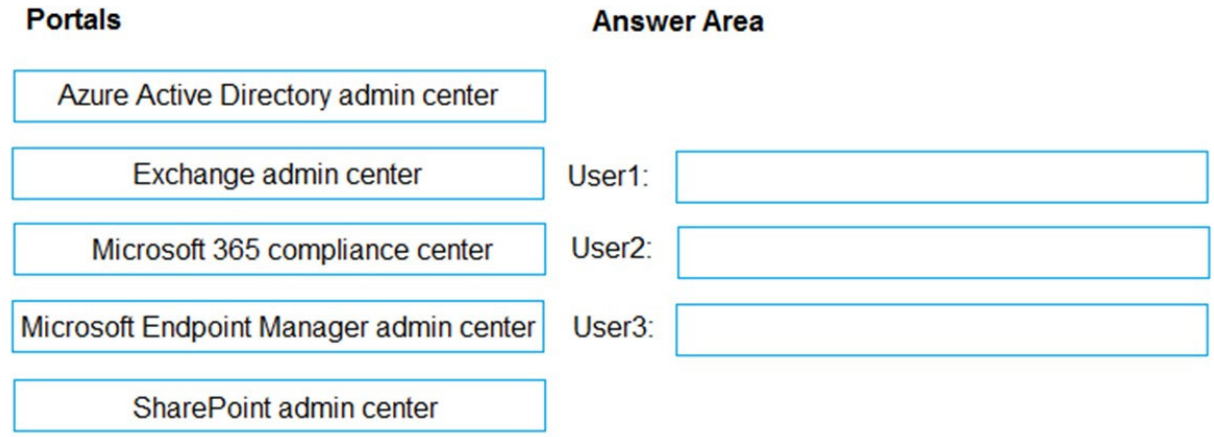
You need to configure the users as shown in the following table.

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

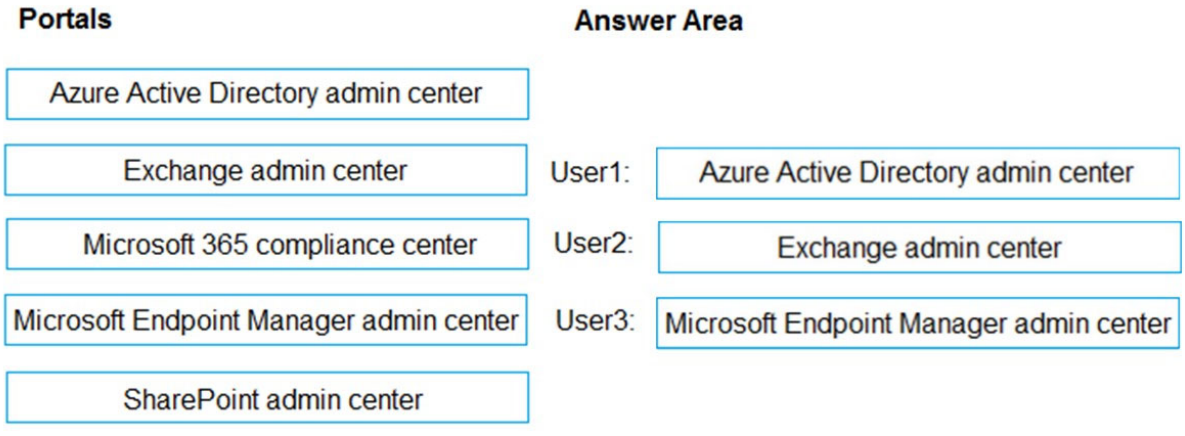
Which portal should you use to configure each user? To answer, drag the appropriate portals to the correct users. Each portal may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Correct Answer:



Question #23 *Topic 1*

You have an Active Directory forest that syncs to an Azure Active Directory (Azure AD) tenant. The tenant uses pass-through authentication.
A corporate security policy states the following:
- Domain controllers must never communicate directly to the internet.
- Only required software must be installed on servers.

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

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

You need to ensure that users can authenticate to Azure AD if a server fails.
On which server should you install an additional pass-through authentication agent?

A. Server4

B. Server2

C. Server1

D. Server3

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

Community vote distribution
A (93%) 7%

Question #24 *Topic 1*

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

A. Run the New-AzureADMSInvitation cmdlet.

B. Configure the External collaboration settings.

C. Add a WS-Fed identity provider.

D. Implement Azure AD Connect.

Correct Answer: *A*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-add-guest-users-portal
https://docs.microsoft.com/en-us/powershell/module/azuread/new-azureadmsinvitation?view=azureadps-2.0

Community vote distribution
A (77%) B (23%)

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

A. the Administrative units blade in the Azure Active Directory admin center

B. the Set-AzureAdUser cmdlet

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

D. the Set-MsolUserLicense cmdlet

Correct Answer: *D*
The Set-MsolUserLicense cmdlet updates the license assignment for a user. This can include adding a new license, removing a license, updating the license options, or any combination of these actions.
Note:
There are several versions of this question in the exam. The question has two possible correct answers:
1. the Licenses blade in the Azure Active Directory admin center
2. the Set-MsolUserLicense cmdlet
Other incorrect answer options you may see on the exam include the following:
- the Identity Governance blade in the Azure Active Directory admin center
- the Set-WindowsProductKey cmdlet
- the Set-AzureAdGroup cmdlet
Reference:
https://docs.microsoft.com/en-us/powershell/module/msonline/set-msoluserlicense?view=azureadps-1.0

Community vote distribution

D (100%)

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:

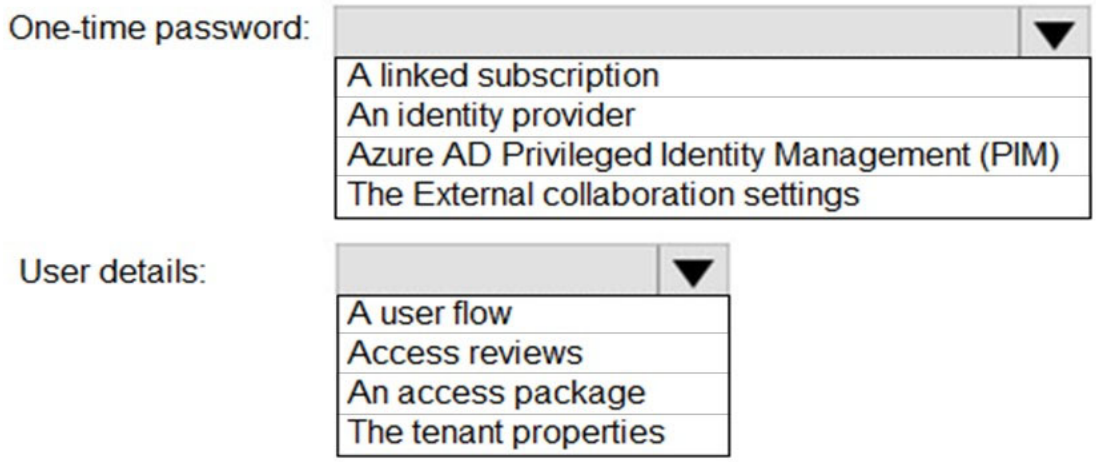
- Guest users must be able to sign up by using a one-time password.
- The users must provide their first name, last name, city, and email address during the sign-up process.

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.

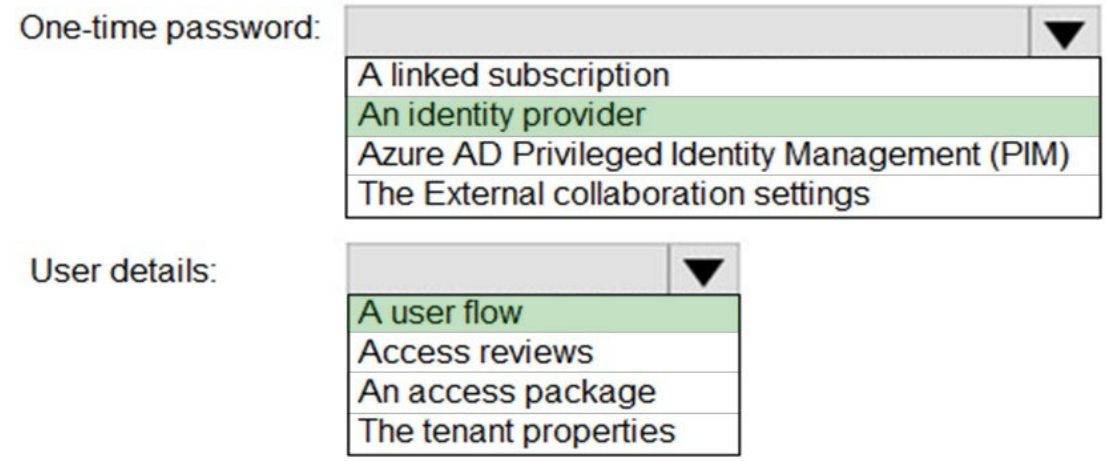
Hot Area:

Answer Area



Correct Answer:

Answer Area



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 *Topic 1*

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

A. displayName, identityIssuer, usageLocation, and userType

B. accountEnabled, givenName, surname, and userPrincipalName

C. accountEnabled, displayName, userPrincipalName, and passwordProfile

D. accountEnabled, passwordProfile, usageLocation, and userPrincipalName

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

Community vote distribution

C (100%)

Question #28 *Topic 1*

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

A. Configure Sign-in options from the Settings app.

B. Enable Enterprise State Roaming.

C. Modify the Intranet Zone settings.

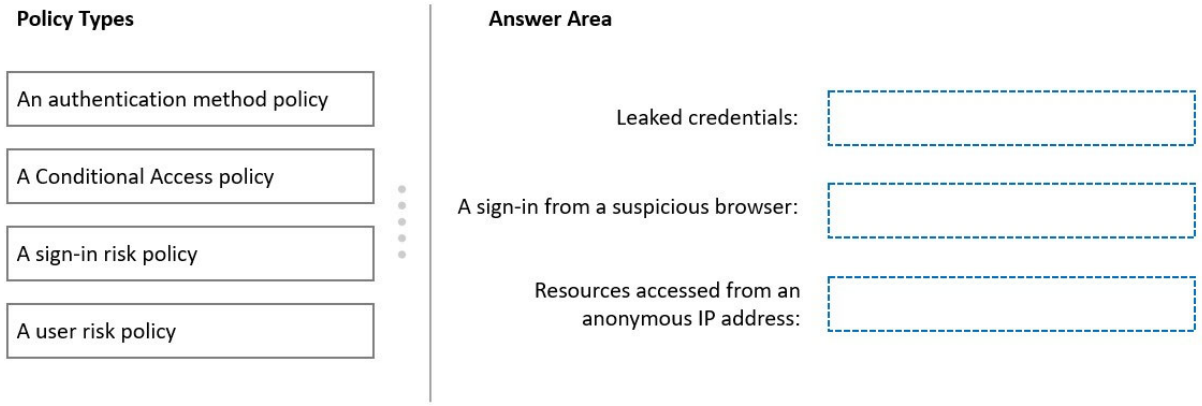
D. Install the Azure AD Connect Authentication Agent.

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

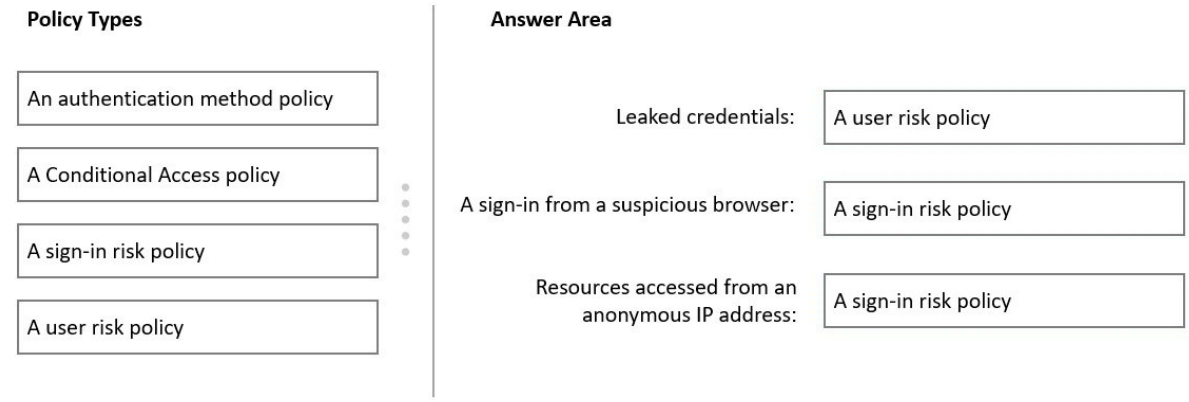
Community vote distribution

C (100%)

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:



Correct Answer:



Box 1: A user risk policy -
User-linked detections include:
Leaked credentials: This risk detection type indicates that the user's valid credentials have been leaked. When cybercriminals compromise valid passwords of legitimate users, they often share those credentials.
User risk policy.
Identity Protection can calculate what it believes is normal for a user's behavior and use that to base decisions for their risk. User risk is a calculation of probability that an identity has been compromised. Administrators can make a decision based on this risk score signal to enforce organizational requirements. Administrators can choose to block access, allow access, or allow access but require a password change using Azure AD self-service password reset.

Box 2: A sign-in risk policy -
Suspicious browser: Suspicious browser detection indicates anomalous behavior based on suspicious sign-in activity across multiple tenants from different countries in the same browser.

Box 3: A sign-in risk policy -
A sign-in risks include activity from anonymous IP address: This detection is discovered by Microsoft Defender for Cloud Apps. This detection identifies that users were active from an IP address that has been identified as an anonymous proxy IP address.
Note: The following three policies are available in Azure AD Identity Protection to protect users and respond to suspicious activity. You can choose to turn the policy enforcement on or off, select users or groups for the policy to apply to, and decide if you want to block access at sign-in or prompt for additional action.
* User risk policy

Identifies and responds to user accounts that may have compromised credentials. Can prompt the user to create a new password.
* Sign in risk policy
Identifies and responds to suspicious sign-in attempts. Can prompt the user to provide additional forms of verification using Azure AD Multi-Factor Authentication.
* MFA registration policy
Makes sure users are registered for Azure AD Multi-Factor Authentication. If a sign-in risk policy prompts for MFA, the user must already be registered for Azure
AD Multi-Factor Authentication.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies

HOTSPOT -

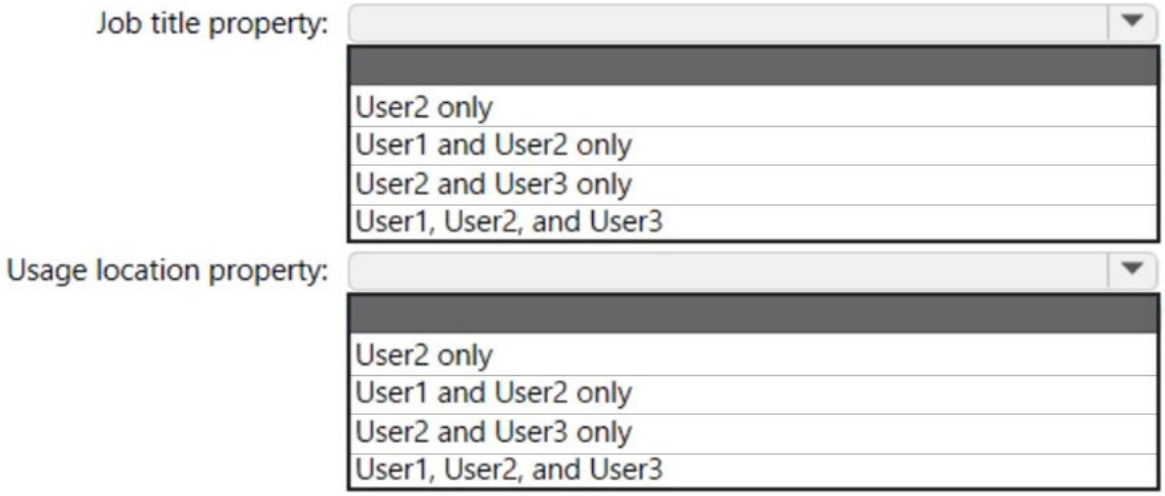
You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

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

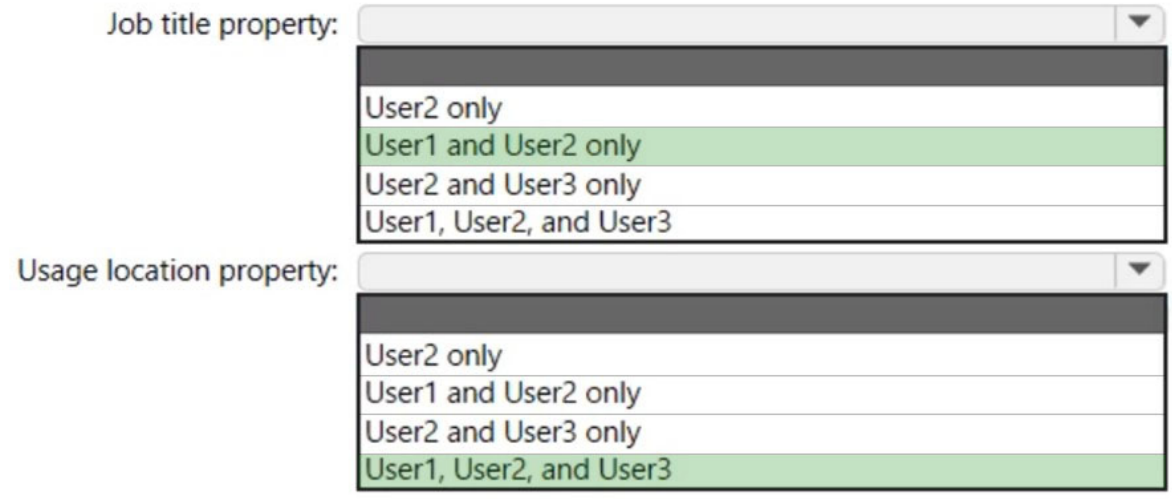
For which users can you configure the Job title property and the Usage location property in Azure AD? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Box 1: User1 and User2 only.

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

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

The user profile includes:

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

Box 2: User1, User2, and User3 -

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

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

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

2. Click on the invited user, and then click Profile.
3. Update First name, Last name, and Usage location.
4. Click Save, and then close the Profile blade.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-users-profile-azure-portal
https://docs.microsoft.com/en-us/power-platform/admin/invite-users-azure-active-directory-b2b-collaboration#update-users-name-and-usage-location

Question #31 *Topic 1*

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

A. From the Roles and administrators blade, modify the Groups administrator role.

B. From the Roles and administrators blade, modify the Service support administrator role.

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

D. From the Identity Governance blade, modify the roles and administrators for the General catalog.

Correct Answer: *C*
Create and manage a catalog of resources in Azure AD entitlement management.
Create a catalog.
A catalog is a container of resources and access packages. You create a catalog when you want to group related resources and access packages. A user who has been delegated the catalog creator role can create a catalog for resources that they own. Whoever creates the catalog becomes the first catalog owner. A catalog owner can add more users, groups of users, or application service principals as catalog owners.
Prerequisite roles: Global administrator, Identity Governance administrator, User administrator, or Catalog creator.
Incorrect:
* Groups Administrator - Members of this role can create/manage groups, create/manage groups settings like naming and expiration policies, and view groups activity and audit reports.
* Service Support Administrator
Users with this role can create and manage support requests with Microsoft for Azure and Microsoft 365 services, and view the service dashboard and message center in the Azure portal and Microsoft 365 admin center.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-catalog-create https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

Community vote distribution

C (100%)

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

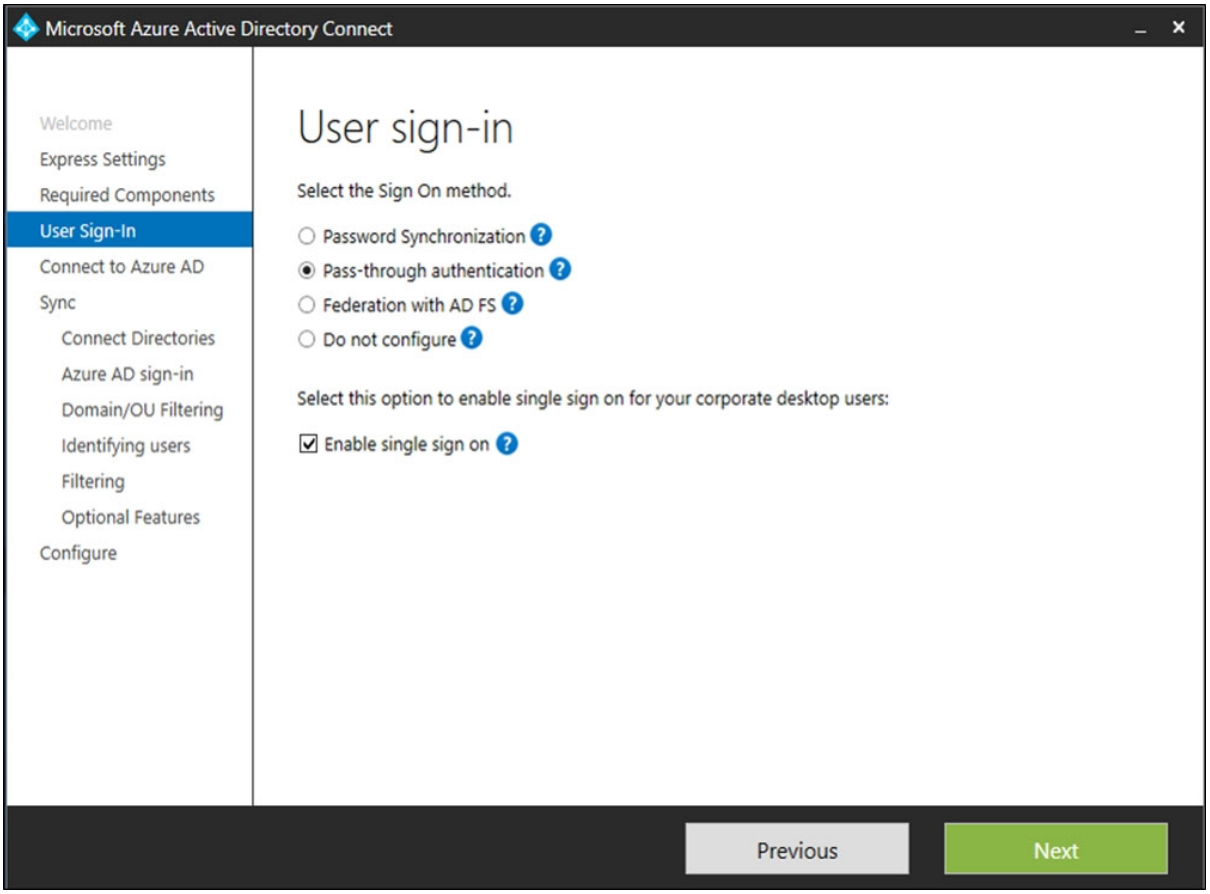
A. Configure Sign-in options from the Settings app.

B. Enable Enterprise State Roaming.

C. Modify the Local intranet Zone settings.

D. Install the Azure AD Connect Authentication Agent.

Correct Answer: *A*
Enable Seamless SSO through Azure AD Connect.
At the User sign-in page, select the Enable single sign on option.

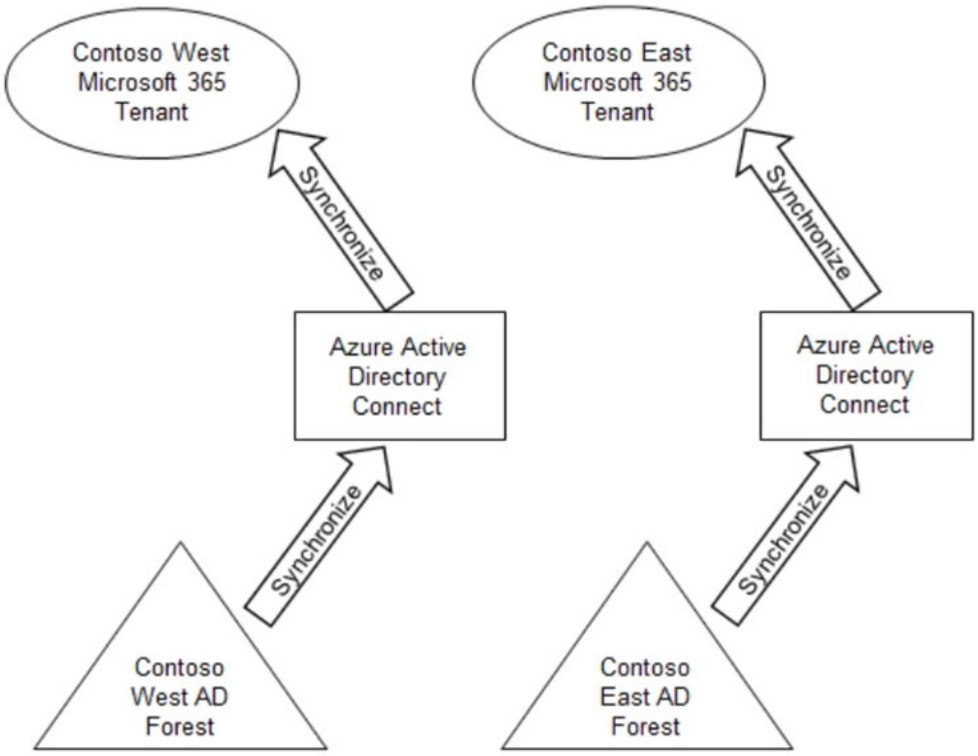


Note:
The option will be available for selection only if the Sign On method is Password Hash Synchronization or Pass-through Authentication.
Seamless SSO can be combined with either the Password Hash Synchronization or Pass-through Authentication sign-in methods.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso-quick-start

Community vote distribution

C (100%)

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



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

A. Configure Azure AD Application Proxy in the Contoso West tenant.

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

C. Deploy a second Azure AD Connect server to Contoso East and configure the server to sync the Contoso East Active Directory forest to the Contoso West tenant.

D. Configure the existing Azure AD Connect server in Contoso East to sync the Contoso East Active Directory forest to the Contoso West tenant.

Correct Answer: *B*
Before any of your users can grant SharePoint Online team site access to external guests, you will have to enable guest sharing from within Azure Active
Directory.
Reference:
https://redmondmag.com/articles/2020/03/11/guest-access-sharepoint-online-team-sites.aspx https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/multi-tenant-common-considerations

Community vote distribution

B (100%)

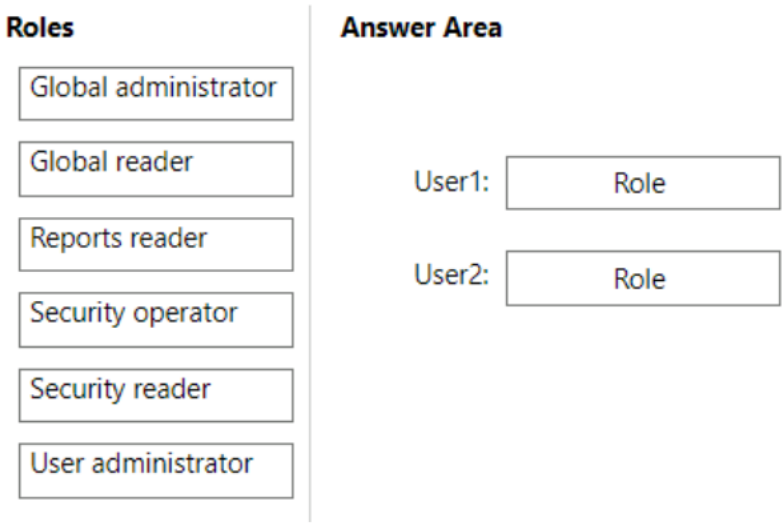
DRAG DROP
-

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

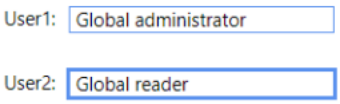
You need to ensure that User1 can create access reviews for groups, and that User2 can review the history report for all the completed access reviews. The solution must use the principle of least privilege.

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.



Correct Answer:



HOTSPOT
-

You have an Azure subscription.

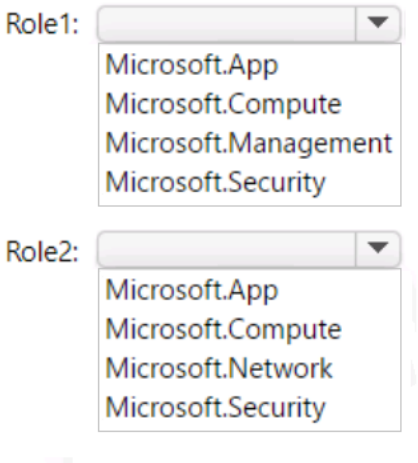
You need to create two custom roles named Role1 and Role2. The solution must meet the following requirements:

• 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



Correct Answer:

Role1: Microsoft.Compute

Role2: Microsoft.Security

HOTSPOT
-

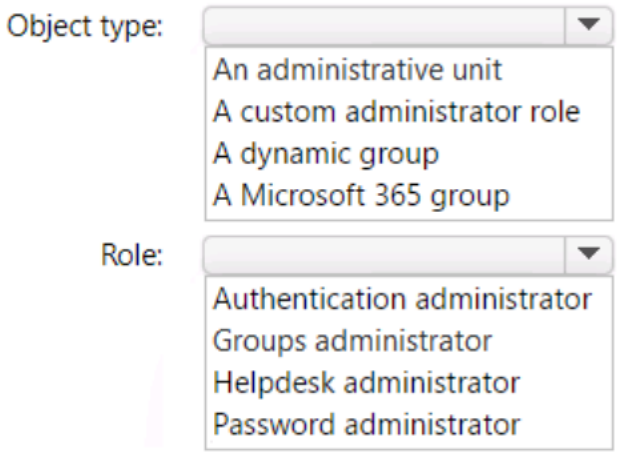
You have a Microsoft 365 tenant that has 5,000 users. One hundred of the users are executives. The executives have a dedicated support team.

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



Correct Answer:

Object type: A custom administrator role

Role: Helpdesk administrator

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

Name	Group
User1	Group1
User2	Group1
User3	Group2
User4	Group2
User5	*None*

You have an administrative unit named Au1. Group1, User2, and User3 are members of Au1.

User5 is assigned the User administrator role for Au1.

For which users can User5 reset passwords?

A. User1, User2, and User3

B. User1 and User2 only

C. User3 and User4 only

D. User2 and User3 only

Correct Answer: *D*

Community vote distribution

D (100%)

Question #38 *Topic 1*

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

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

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

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

Which users will be added to the group?

A. User1 only

B. User2 only

C. User3 only

D. User1 and User2 only

E. User1 and User3 only

F. User1, User2, and User3

Correct Answer: *D*

Community vote distribution

D (58%) A (42%)

Question #39 *Topic 1*

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

User1 needs to manage license assignments and reset user passwords.

Which role should you assign to User1?

A. Helpdesk administrator

B. Billing administrator

C. License administrator

D. User administrator

Correct Answer: *D*

Community vote distribution

D (100%)

Question #40 *Topic 1*

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

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

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

What should you use?

A. the Set-MsolUserLicense cmdlet

B. the Set-AzureADGroup cmdlet

C. the Set-WindowsProductKey cmdlet

D. the Administrative units blade in the Azure Active Directory admin center

Correct Answer: *D*

Community vote distribution

A (100%)

Question #41 *Topic 1*

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

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

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

What should you use?

A. the Set-AzureADGroup cmdlet

B. the Identity Governance blade in the Azure Active Directory admin center

C. the Set-WindowsProductKey cmdlet

D. the Set-MsolUserLicense cmdlet

Correct Answer: *B*

Community vote distribution

D (100%)

HOTSPOT
-

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

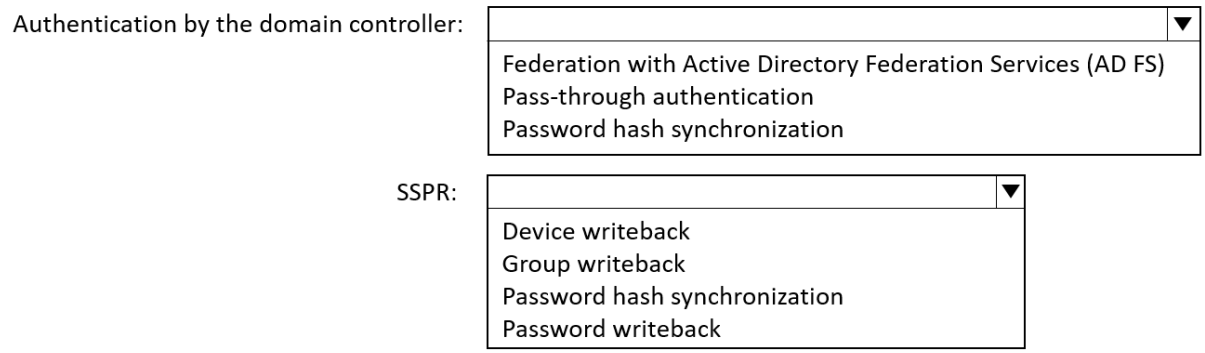
You need to configure Azure AD Connect to meet the following requirements:

• 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.

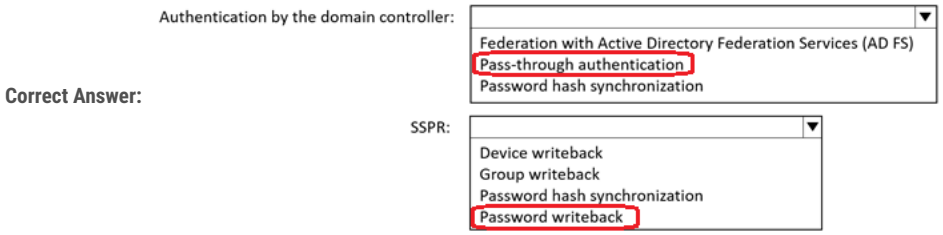
NOTE: Each correct selection is worth one point.

Answer Area



Correct Answer:

Answer Area



Question #43 *Topic 1*

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

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

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

What should you use?

A. the Groups blade in the Azure Active Directory admin center

B. the Set-AzureADGroup cmdlet

C. the Identity Governance blade in the Azure Active Directory admin center

D. the Set-MsolUserLicense cmdlet

Correct Answer: *D*

Question #44 *Topic 1*

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

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

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

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

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

Solution: You configure conditional access policies.

Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*

Question #45 *Topic 1*

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

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

You have a Microsoft 365 E5 subscription.

You create a user named User1.

You need to ensure that User1 can update the status of Identity Secure Score improvement actions.

Solution: You assign the Exchange Administrator role to User1.

Does this meet the goal?

A. Yes

B. No

Correct Answer: *A*

Question #46 *Topic 1*

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

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

You have a Microsoft 365 E5 subscription.

You create a user named User1.

You need to ensure that User1 can update the status of Identity Secure Score improvement actions.

Solution: You assign the User Administrator role to User1.

Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*

Topic 2 - Question Set 2

Question #1 *Topic 2*

You configure a new Microsoft 365 tenant to use a default domain name of contoso.com.
You need to ensure that you can control access to Microsoft 365 resources by using conditional access policies.
What should you do first?

A. Disable the User consent settings.

B. Disable Security defaults.

C. Configure a multi-factor authentication (MFA) registration policy.

D. Configure password protection for Windows Server Active Directory.

Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults

Question #2 *Topic 2*

Your company has a Microsoft 365 tenant.
The company has a call center that contains 300 users. In the call center, the users share desktop computers and might use a different computer every day. The call center computers are NOT configured for biometric identification.
The users are prohibited from having a mobile phone in the call center.
You need to require multi-factor authentication (MFA) for the call center users when they access Microsoft 365 services.
What should you include in the solution?

A. a named network location

B. the Microsoft Authenticator app

C. Windows Hello for Business authentication

D. FIDO2 tokens

Correct Answer: *D*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordless

Question #3 *Topic 2*

You have an Azure Active Directory (Azure AD) tenant named contoso.com.
All users who run applications registered in Azure AD are subject to conditional access policies.
You need to prevent the users from using legacy authentication.
What should you include in the conditional access policies to filter out legacy authentication attempts?

A. a cloud apps or actions condition

B. a user risk condition

C. a client apps condition

D. a sign-in risk condition

Correct Answer: *C*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacy-authentication

Question #4 *Topic 2*

You have an Azure Active Directory (Azure AD) tenant.
You open the risk detections report.
Which risk detection type is classified as a user risk?

A. impossible travel

B. anonymous IP address

C. atypical travel

D. leaked credentials

Correct Answer: *D*
Leaked credentials indicates that the user's valid credentials have been leaked.
Note:
There are several versions of this question in the exam. The question can have other incorrect answer options, including the following:
- password spray
- malicious IP address
- unfamiliar sign-in properties

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

Question #5 *Topic 2*

You have a Microsoft 365 tenant.
All users have computers that run Windows 10. Most computers are company-owned and joined to Azure Active Directory (Azure AD). Some computers are user- owned and are only registered in Azure AD.
You need to prevent users who connect to Microsoft SharePoint Online on their user-owned computer from downloading or syncing files. Other users must NOT be restricted.
Which policy type should you create?

A. a Microsoft Cloud App Security activity policy that has Microsoft Office 365 governance actions configured

B. an Azure AD conditional access policy that has session controls configured

C. an Azure AD conditional access policy that has client apps conditions configured

D. a Microsoft Cloud App Security app discovery policy that has governance actions configured

Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/proxy-intro-aad

Question #6 *Topic 2*

You have an Active Directory domain that syncs to an Azure Active Directory (Azure AD) tenant.
The on-premises network contains a VPN server that authenticates to the on-premises Active Directory domain. The VPN server does NOT support Azure Multi-
Factor Authentication (MFA).
You need to recommend a solution to provide Azure MFA for VPN connections.
What should you include in the recommendation?

A. Azure AD Application Proxy

B. an Azure AD Password Protection proxy

C. Network Policy Server (NPS)

D. a pass-through authentication proxy

Correct Answer: *C*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-nps-extension-vpn

You have a Microsoft 365 tenant.

The Azure Active Directory (Azure AD) tenant is configured to sync with an on-premises Active Directory domain. The domain contains the servers shown in the following table.

Name	Operating system	Configuration
Server1	Windows Server 2019	Domain controller
Server2	Windows Server 2016	Domain controller
Server3	Windows Server 2019	Azure AD Connect

The domain controllers are prevented from communicating to the internet.

You implement Azure AD Password Protection on Server1 and Server2.

You deploy a new server named Server4 that runs Windows Server 2019.

You need to ensure that Azure AD Password Protection will continue to work if a single server fails.

What should you implement on Server4?

A. Azure AD Connect

B. Azure AD Application Proxy

C. Password Change Notification Service (PCNS)

D. the Azure AD Password Protection proxy service

Correct Answer: *D*

Reference:

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

DRAG DROP -

You have a Microsoft 365 E5 tenant.

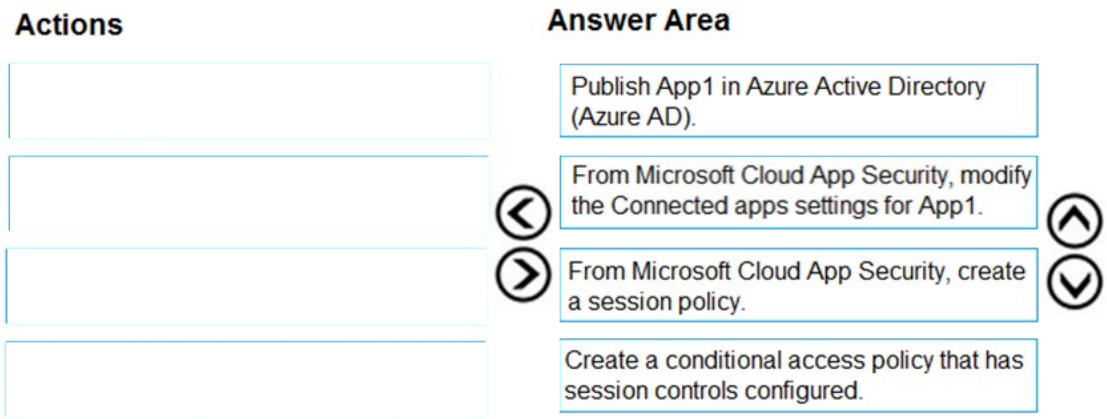
You purchase a cloud app named App1.

You need to enable real-time session-level monitoring of App1 by using Microsoft Cloud App Security.

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

Select and Place:

Correct Answer:



Reference:

https://docs.microsoft.com/en-us/cloud-app-security/proxy-deployment-any-app https://docs.microsoft.com/en-us/cloud-app-security/session-policy-aad

Question #9 *Topic 2*

You have a Microsoft 365 tenant.
All users have mobile phones and laptops.
The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity. While working from the remote locations, the users connect their laptop to a wired network that has internet access.
You plan to implement multi-factor authentication (MFA).
Which MFA authentication method can the users use from the remote location?

A. a notification through the Microsoft Authenticator app

B. an app password

C. Windows Hello for Business

D. SMS

Correct Answer: *C*
In Windows 10, Windows Hello for Business replaces passwords with strong two-factor authentication on PCs and mobile devices. This authentication consists of a new type of user credential that is tied to a device and uses a biometric or PIN.
After an initial two-step verification of the user during enrollment, Windows Hello is set up on the user's device and Windows asks the user to set a gesture, which can be a biometric, such as a fingerprint, or a PIN. The user provides the gesture to verify their identity. Windows then uses Windows Hello to authenticate users.
Incorrect Answers:
A: A notification through the Microsoft Authenticator app requires connectivity to send the verification code to the device requesting the logon
B: An app password can be used to open an application but it cannot be used to sign in to a computer.

D: SMS requires a mobile phone -
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-overview

Question #10 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 tenant.
All users must use the Microsoft Authenticator app for multi-factor authentication (MFA) when accessing Microsoft 365 services.
Some users report that they received an MFA prompt on their Microsoft Authenticator app without initiating a sign-in request.
You need to block the users automatically when they report an MFA request that they did not initiate.
Solution: From the Azure portal, you configure the Notifications settings for multi-factor authentication (MFA).
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
You need to configure the fraud alert settings.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings

Question #11 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 tenant.
All users must use the Microsoft Authenticator app for multi-factor authentication (MFA) when accessing Microsoft 365 services.
Some users report that they received an MFA prompt on their Microsoft Authenticator app without initiating a sign-in request.
You need to block the users automatically when they report an MFA request that they did not initiate.
Solution: From the Azure portal, you configure the Account lockout settings for multi-factor authentication (MFA).
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
You need to configure the fraud alert settings.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings

Question #12 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 tenant.
All users must use the Microsoft Authenticator app for multi-factor authentication (MFA) when accessing Microsoft 365 services.
Some users report that they received an MFA prompt on their Microsoft Authenticator app without initiating a sign-in request.
You need to block the users automatically when they report an MFA request that they did not initiate.
Solution: From the Azure portal, you configure the Block/unblock users settings for multi-factor authentication (MFA).
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
You need to configure the fraud alert settings.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings

HOTSPOT -

You have a Microsoft 365 tenant.

You need to identify users who have leaked credentials. The solution must meet the following requirements:

- Identify sign-ins by users who are suspected of having leaked credentials.
- Flag the sign-ins as a high-risk event.
- Immediately enforce a control to mitigate the risk, while still allowing the user to access applications.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

To classify leaked credentials as high-risk, use:
- Azure Active Directory (Azure AD) Identity Protection
- Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
- Identity Governance
- Self-service password reset (SSPR)

To trigger remediation, use:
- Client apps not using Modern authentication
- Device state
- Sign-in risk
- User location
- User risk

To mitigate the risk, select:
- Apply app enforced restrictions
- Block access
- Grant access but require app protection policy
- Grant access but require password change

Correct Answer:

Answer Area

To classify leaked credentials as high-risk, use:
- Azure Active Directory (Azure AD) Identity Protection
- Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
- Identity Governance
- Self-service password reset (SSPR)

To trigger remediation, use:
- Client apps not using Modern authentication
- Device state
- Sign-in risk
- User location
- User risk

To mitigate the risk, select:
- Apply app enforced restrictions
- Block access
- Grant access but require app protection policy
- Grant access but require password change

Reference:

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

HOTSPOT -

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

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

You plan to implement Azure AD Identity Protection.

Which users can configure the user risk policy, and which users can view the risky users report? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Configure the user risk policy:
- User3 only
- User3 and User4 only
- User1, User2, and User3 only
- User1, User3, and User4 only
- User1, User2, User3, and User4

View the risky users report:
- User3 only
- User3 and User4 only
- User1, User2, and User3 only
- User1, User3, and User4 only
- User1, User2, User3, and User4

Correct Answer:

Answer Area

Configure the user risk policy:
- User3 only
- User3 and User4 only
- User1, User2, and User3 only
- User1, User3, and User4 only
- User1, User2, User3, and User4

View the risky users report:
- User3 only
- User3 and User4 only
- User1, User2, and User3 only
- User1, User3, and User4 only
- User1, User2, User3, and User4

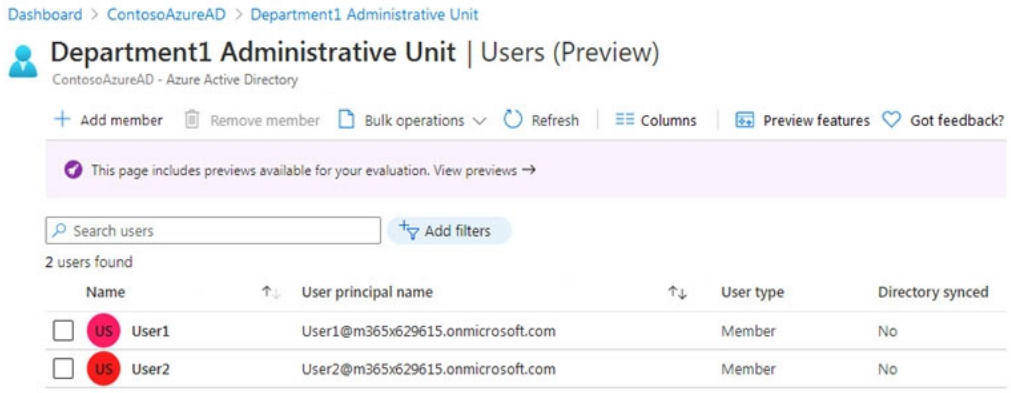
Reference:

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

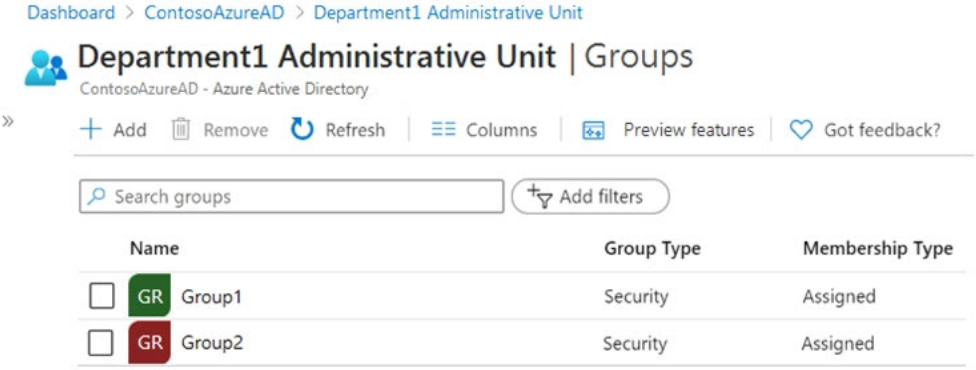
HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant that contains a group named Group3 and an administrative unit named Department1.

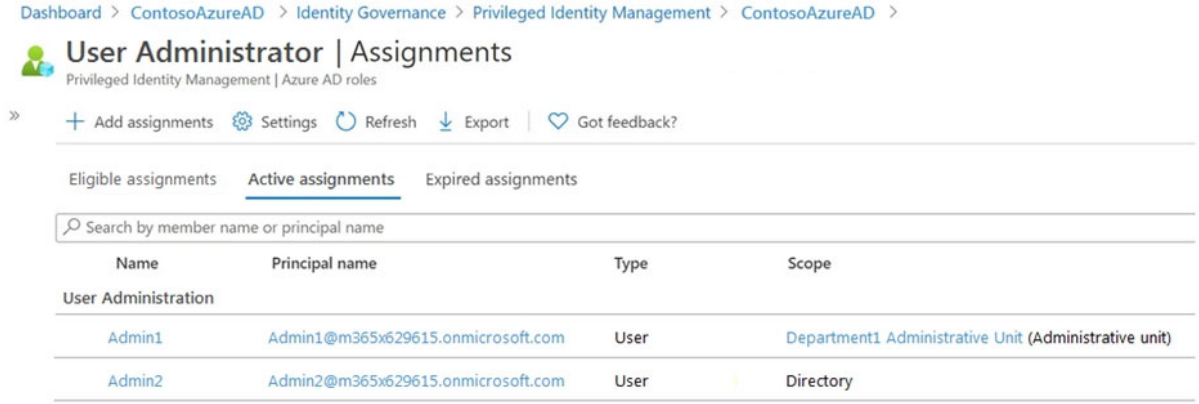
Department1 has the users shown in the Users exhibit. (Click the Users tab.)



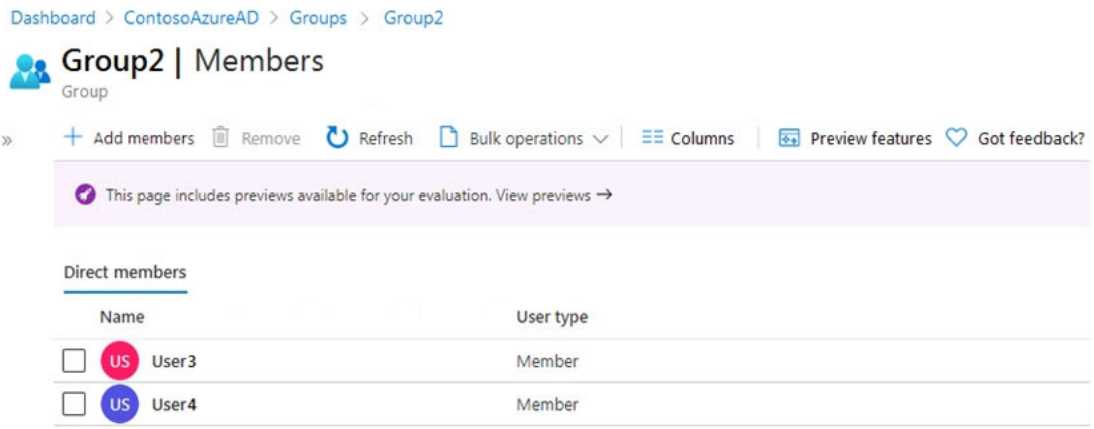
Department1 has the groups shown in the Groups exhibit. (Click the Groups tab.)



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



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



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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

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

Correct Answer:

Answer Area

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

Reference:

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

Question #16 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 tenant.
All users must use the Microsoft Authenticator app for multi-factor authentication (MFA) when accessing Microsoft 365 services.
Some users report that they received an MFA prompt on their Microsoft Authenticator app without initiating a sign-in request.
You need to block the users automatically when they report an MFA request that they did not initiate.
Solution: From the Azure portal, you configure the Fraud alert settings for multi-factor authentication (MFA).
Does this meet the goal?

A. Yes

B. No

Correct Answer: *A*
The fraud alert feature lets users report fraudulent attempts to access their resources. When an unknown and suspicious MFA prompt is received, users can report the fraud attempt using the Microsoft Authenticator app or through their phone.
The following fraud alert configuration options are available:
- Automatically block users who report fraud.
- Code to report fraud during initial greeting.

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

Question #17 *Topic 2*

You have a Microsoft 365 tenant.
All users have mobile phones and laptops.
The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity. While working from the remote locations, the users connect their laptop to a wired network that has internet access.
You plan to implement multi-factor authentication (MFA).
Which MFA authentication method can the users use from the remote location?

A. a notification through the Microsoft Authenticator app

B. email

C. security questions

D. a verification code from the Microsoft Authenticator app

Correct Answer: *D*
The Authenticator app can be used as a software token to generate an OATH verification code. After entering your username and password, you enter the code provided by the Authenticator app into the sign-in interface.
Incorrect Answers:
A: A notification through the Microsoft Authenticator app requires connectivity to send the verification code to the device requesting the logon.
B: An email requires network connectivity.
C: Security questions are not used as an authentication method but can be used during the self-service password reset (SSPR) process.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-authenticator-app#verification-code-from-mobile-app

HOTSPOT -

You have a Microsoft 365 tenant.

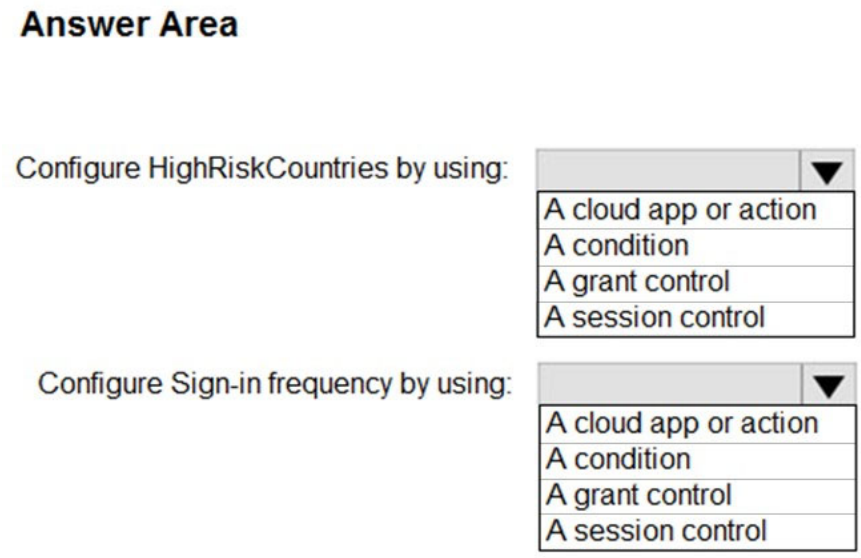
You create a named location named HighRiskCountries that contains a list of high-risk countries.

You need to limit the amount of time a user can stay authenticated when connecting from a high-risk country.

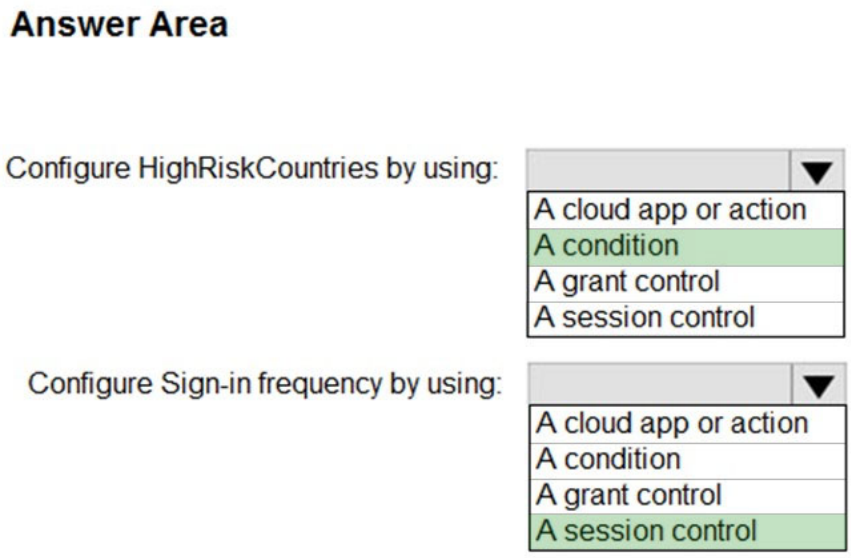
What should you configure in a conditional access policy? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Reference:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session

HOTSPOT -

A user named User1 attempts to sign in to the tenant by entering the following incorrect passwords:

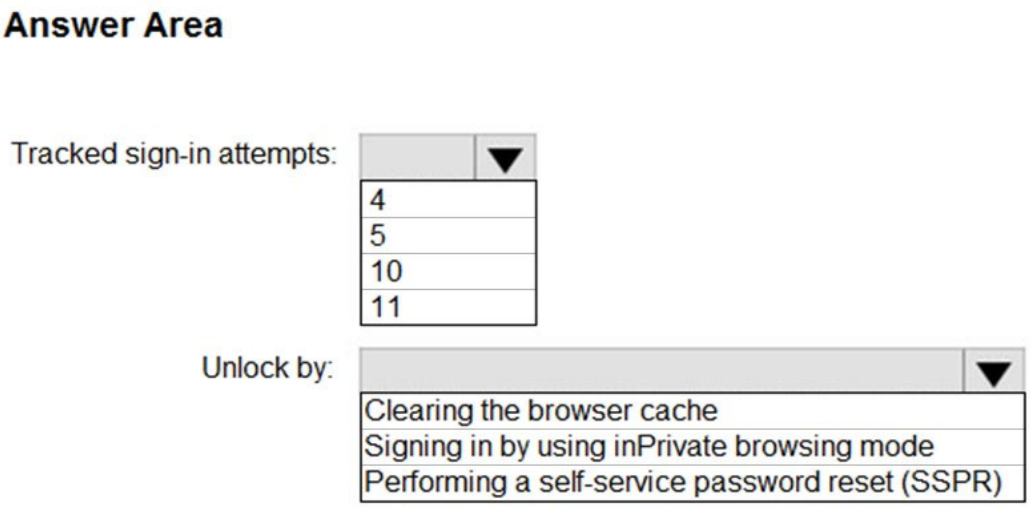
- Pa55w0rd12
- Pa55w0rd12
- Pa55w0rd12
- Pa55w.rd12
- Pa55w.rd123
- Pa55w.rd123
- Pa55w.rd123
- Pa55word12
- Pa55word12
- Pa55word12
- Pa55w.rd12

You need to identify how many sign-in attempts were tracked for User1, and how User1 can unlock her account before the 300-second lockout duration expires.

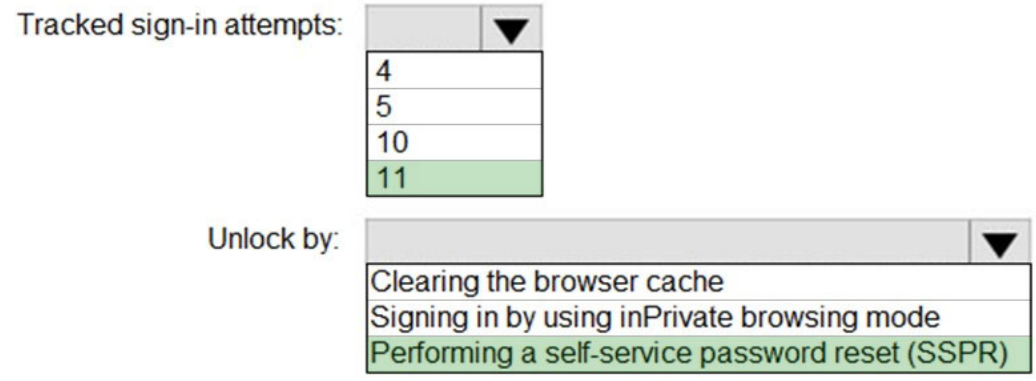
What should identify? To answer, select the appropriate

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



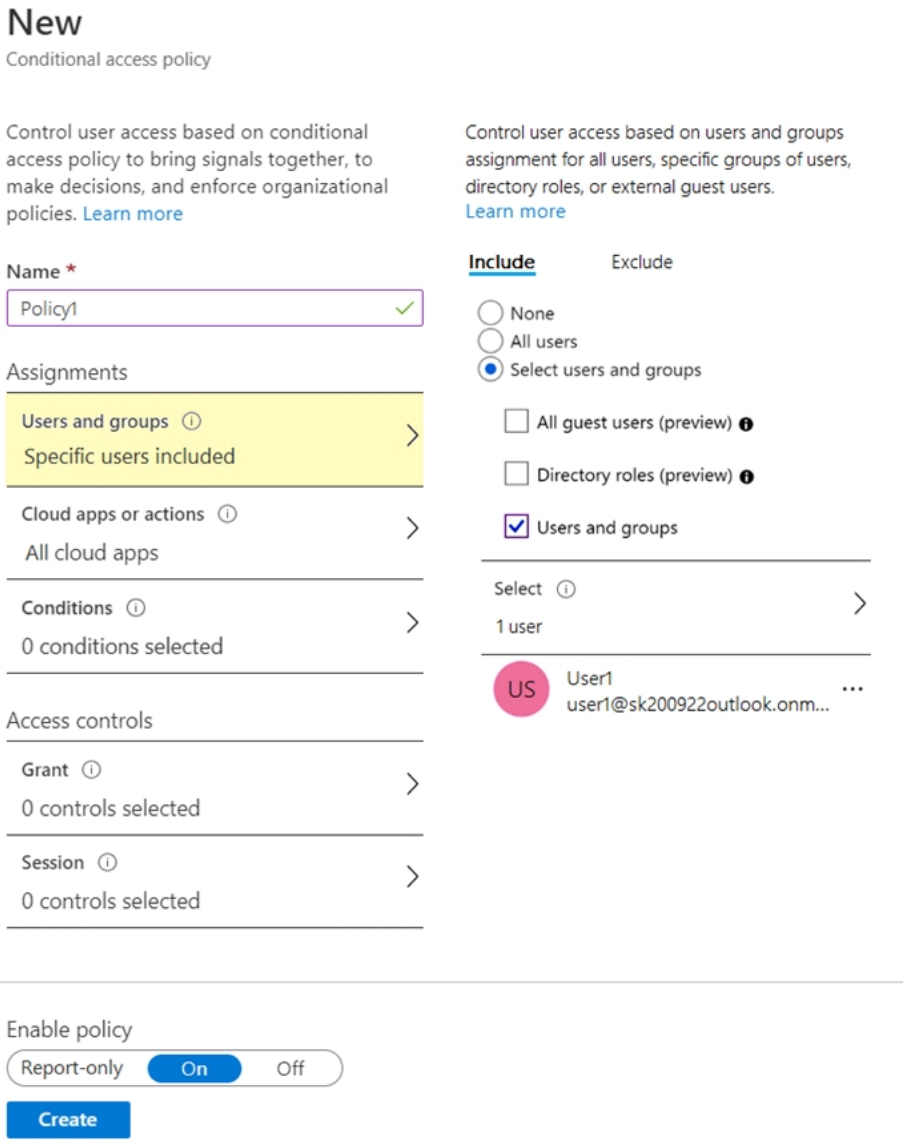
Reference:

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

HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant that has Security defaults disabled.

You are creating a conditional access policy as shown in the following exhibit.



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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

To ensure that User1 is prompted for multi-factor authentication (MFA) when accessing Cloud apps, you must configure the **[answer choice]**.

- Conditions settings
- Enable policy setting
- Grant settings
- Sessions settings
- Users and groups setting

To ensure that User1 is prompted for authentication every eight hours, you must configure the **[answer choice]**.

- Conditions settings
- Enable policy setting
- Grant settings
- Sessions settings
- Users and groups setting

Answer Area

To ensure that User1 is prompted for multi-factor authentication (MFA) when accessing Cloud apps, you must configure the **[answer choice]**.

- Conditions settings
- Enable policy setting
- Grant settings
- Sessions settings
- Users and groups setting

Correct Answer:

To ensure that User1 is prompted for authentication every eight hours, you must configure the **[answer choice]**.

- Conditions settings
- Enable policy setting
- Grant settings
- Sessions settings
- Users and groups setting

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

Question #21 *Topic 2*

You have an Azure Active Directory (Azure AD) tenant that contains a user named SecAdmin1. SecAdmin1 is assigned the Security administrator role.
SecAdmin1 reports that she cannot reset passwords from the Azure AD Identity Protection portal.
You need to ensure that SecAdmin1 can manage passwords and invalidate sessions on behalf of non-administrative users. The solution must use the principle of least privilege.
Which role should you assign to SecAdmin1?

A. Authentication administrator

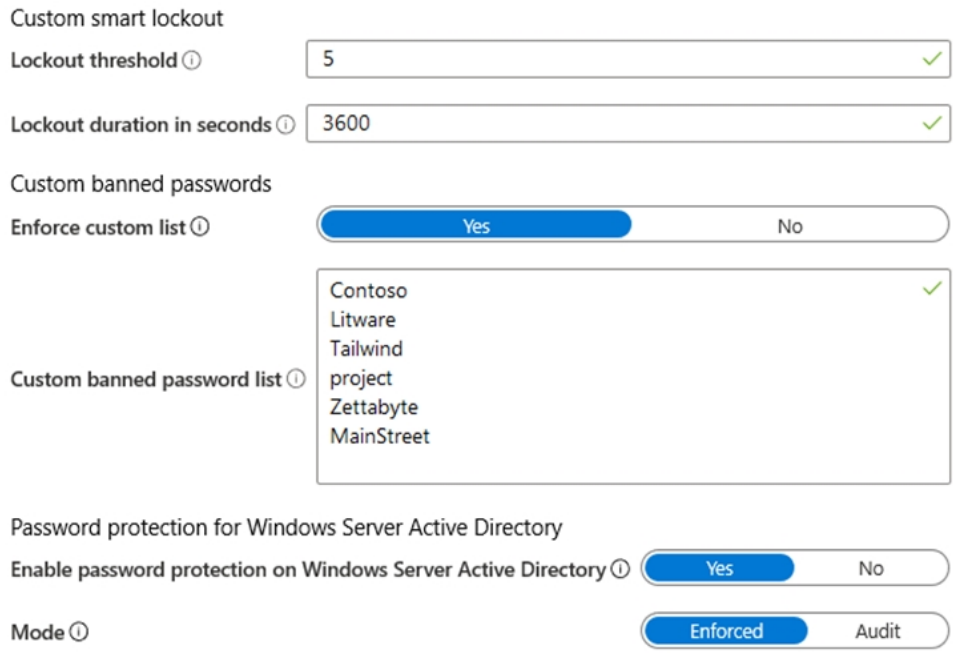
B. Helpdesk administrator

C. Privileged authentication administrator

D. Security operator

Correct Answer: *C*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

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



You are evaluating the following passwords:

- Pr0jectlitw@re
- T@ilw1nd
- C0nt0s0

Which passwords will be blocked?

A. Pr0jectlitw@re and T@ilw1nd only

B. C0nt0s0 only

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

D. C0nt0s0 and T@ilw1nd only

E. C0nt0s0 and Pr0jectlitw@re only

Correct Answer: *C*

Reference:

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

You have a Microsoft 365 tenant.
All users have mobile phones and laptops.
The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity. While working from the remote locations, the users connect their laptop to a wired network that has internet access.
You plan to implement multi-factor authentication (MFA).
Which MFA authentication method can the users use from the remote location?

A. a verification code from the Microsoft Authenticator app

B. security questions

C. voice

D. SMS

Correct Answer: *A*
The Authenticator app can be used as a software token to generate an OATH verification code. After entering your username and password, you enter the code provided by the Authenticator app into the sign-in interface.
Incorrect Answers:
B: Security questions are not used as an authentication method but can be used during the self-service password reset (SSPR) process.
C, D: An automated voice call and an SMS requires mobile connectivity.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods

HOTSPOT -

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

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

User2 reports that he can only configure multi-factor authentication (MFA) to use the Microsoft Authenticator app.

You need to ensure that User2 can configure alternate MFA methods.

Which configuration is required, and which user should perform the configuration? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

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

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

Answer Area

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

Correct Answer:

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

Box 1: Modify security defaults.

Privileged Authentication Administrator

Users with this role can set or reset any authentication method (including passwords) for any user, including Global Administrators. Privileged Authentication

Administrators can force users to re-register against existing non-password credential (such as MFA or FIDO) and revoke 'remember MFA on the device', prompting for MFA on the next sign-in of all users.
The Authentication Administrator role has permission to force re-registration and multifactor authentication for standard users and users with some admin roles.

Role	Manage user's auth methods	Manage per-user MFA	Manage MFA settings	Manage auth method policy	Manage password protection policy
Authentication Administrator	Yes for some users (see above)	Yes for some users (see above)	No	No	No
Privileged Authentication Administrator	Yes for all users	Yes for all users	No	No	No
Authentication Policy Administrator	No	No	Yes	Yes	Yes

Box 2: User1 only.
Security Administrator.
Users with this role have permissions to manage security-related features in the Microsoft 365 Defender portal, Azure Active Directory Identity Protection, Azure
Active Directory Authentication, Azure Information Protection, and Office 365 Security & Compliance Center.
Incorrect:
Not User3. Service Support Administrator.
Users with this role can create and manage support requests with Microsoft for Azure and Microsoft 365 services, and view the service dashboard and message center in the Azure portal and Microsoft 365 admin center.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

Question #25 *Topic 2*

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

What is a valid authentication method available to users?

A. a Microsoft Teams chat
B. a mobile app notification
C. a mobile app code
D. an FIDO2 security token

Correct Answer: *C*
When administrators require one method be used to reset a password, verification code is the only option available.
Note: When administrators require two methods be used to reset a password, users are able to use notification OR verification code in addition to any other enabled methods.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks

You have an Azure Active Directory (Azure AD) tenant that uses Azure AD Identity Protection and contains the resources shown in the following table.

Name	Type	Configuration
Risk1	User risk policy	Users that have a high severity risk must reset their password upon next sign-in.
User1	User	*Not applicable*

Azure Multi-factor Authentication (MFA) is enabled for all users.

User1 triggers a medium severity alert that requires additional investigation.

You need to force User1 to reset his password the next time he signs in. The solution must minimize administrative effort.

What should you do?

A. Reconfigure the user risk, policy to trigger on medium or low severity.

B. Mark User1 as compromised.

C. Reset the Azure MIFA registration for User1.

D. Configure a sign-in risk policy.

Correct Answer: *B*

Scenario: User compromised (True positive)

'Risky users' report shows an at-risk user [Risk state = At risk] with low risk [Risk level = Low] and that user was indeed compromised.

Feedback: Select the user and click on 'Confirm user compromised'.

What happens under the hood? Azure AD will move the user risk to High [Risk state = Confirmed compromised; Risk level = High] and will add a new detection

'Admin confirmed user compromised'.

Notes: Currently, the 'Confirm user compromised' option is only available in 'Risky users' report.

The detection 'Admin confirmed user compromised' is shown in the tab 'Risk detections not linked to a sign-in' in the 'Risky users' report.

Reference:

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

HOTSPOT -

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

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

In Azure. AD Identity Protection, you configure a user risk policy that has the following settings:

⇨ Assignments:

- Users: Group1
- User risk: Low and above

⇨ Controls:

- Access: Block access

⇨ Enforce policy: On

In Azure AD Identify Protection, you configure a sign-in risk policy that has the following settings:

⇨ Assignments:

- Users: Group2
- Sign-in risk: Low and above

⇨ Controls:

- Access: Require multi-factor authentication

⇨ Enforce policy: On

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

NOTE: Each correct selection is worth one point.

Hot Area:

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

Correct Answer:

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

Box 1: Yes -

Note: Azure AD Identity Protection can review user sign-in attempts and take additional action if there's suspicious behavior:

Some of the following actions may trigger Azure AD Identity Protection risk detection:

Users with leaked credentials.

* -> Sign-ins from anonymous IP addresses.

Impossible travel to atypical locations.

Sign-ins from infected devices.

Sign-ins from IP addresses with suspicious activity.

Sign-ins from unfamiliar locations.

Box 2: No -

Box 3: No -
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-risk-based-sspr-mfa

Question #28 *Topic 2*

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

What is a valid authentication method available to users?

A. an email to an address outside your organization

B. a smartcard

C. an FID02 security token

D. a Microsoft Teams chat

Correct Answer: *A*
A one-gate policy requires one piece of authentication data, such as an email address or phone number.
A one-gate policy applies in the following circumstances:
It's within the first 30 days of a trial subscription; or
A custom domain hasn't been configured for your Azure AD tenant so is using the default *.onmicrosoft.com. The default *.onmicrosoft.com domain isn't recommended for production use; and Azure AD Connect isn't synchronizing identities.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-policy#administrator-reset-policy-differences

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

Name	Member of
User1	Group1
User2	Group2
User3	Group3

The tenant has the authentication methods shown in the following table.

Method	Target	Enabled
FIDO2	Group2	Yes
Microsoft Authenticator app	Group1	Yes
SMS	Group3	Yes

Which users will sign in to cloud apps by matching a number shown in the app with a number shown on their phone?

A. User1 only

B. User2 only

C. User3 only

D. User1 and User2 only

E. User2 and User3 only

Correct Answer: *A*

Microsoft Authenticator -

You can also allow your employee's phone to become a passwordless authentication method. You may already be using the Authenticator app as a convenient multi-factor authentication option in addition to a password. You can also use the Authenticator App as a passwordless option. The Authenticator App turns any iOS or Android phone into a strong, passwordless credential. Users can sign in to any platform or browser by getting a notification to their phone, matching a number displayed on the screen to the one on their phone, and then using their biometric (touch or face) or PIN to confirm.

Incorrect:

* Not User2

FIDO2 security keys -

The FIDO (Fast IDentity Online) Alliance helps to promote open authentication standards and reduce the use of passwords as a form of authentication. FIDO2 is the latest standard that incorporates the web authentication (WebAuthn) standard.

FIDO2 security keys are an unphishable standards-based passwordless authentication method that can come in any form factor. Fast Identity Online (FIDO) is an open standard for passwordless authentication. FIDO allows users and organizations to leverage the standard to sign in to their resources without a username or password using an external security key or a platform key built into a device.

Reference:

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

Question #30 *Topic 2*

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

Name	Status	Conditional access requirement
CAPolicy1	On	Users connect from a trusted IP address.
CAPolicy2	On	Users' devices are marked as compliant.
CAPolicy3	Report-only	The sign-in risk of users is low.

You need to evaluate which policies will be applied to User1 when User1 attempts to sign-in from various IP addresses.
Which feature should you use?

A. Access reviews

B. Identity Secure Score

C. The What If tool

D. the Microsoft 365 network connectivity test tool

Correct Answer: *C*
The Azure AD conditional access What if tool allows you to understand the impact of your conditional access policies on your environment. Instead of test driving your policies by performing multiple sign-ins manually, this tool enables you to evaluate a simulated sign-in of a user. The simulation estimates the impact this sign-in has on your policies and generates a simulation report. The report does not only list the applied conditional access policies but also classic policies if they exist.
Reference:
https://azure.microsoft.com/en-us/updates/azure-ad-conditional-access-what-if-tool-is-now-available

Question #31 *Topic 2*

You have a Microsoft 365 tenant.
All users have mobile phones and Windows 10 laptops.
The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity. While working from the remote locations, the users connect their laptops to a wired network that has internet access.
You plan to implement multi-factor authentication (MFA).
Which MFA authentication method can the users use from the remote location?

A. an app password

B. voice

C. Windows Hello for Business

D. security questions

Correct Answer: *A*
The Microsoft Authenticator app provides an additional level of security to your Azure AD work or school account or your Microsoft account and is available for
Android and iOS. With the Microsoft Authenticator app, users can authenticate in a passwordless way during sign-in, or as an additional verification option during self-service password reset (SSPR) or multifactor authentication events.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-authenticator-app#verification-code-from-mobile-app

Question #32 *Topic 2*

You create a conditional access policy that blocks access when a user triggers a high-severity sign-in alert.
You need to test the policy under the following conditions:
- A user signs in from another country.
- A user triggers a sign-in risk.

What should you use to complete the test?

A. the Conditional Access What If tool

B. sign-ins logs in Azure Active Directory (Azure AD)

C. the activity logs in Microsoft Defender for Cloud Apps

D. access reviews in Azure Active Directory (Azure AD)

Correct Answer: *A*
The Azure AD conditional access What if tool allows you to understand the impact of your conditional access policies on your environment. Instead of test driving your policies by performing multiple sign-ins manually, this tool enables you to evaluate a simulated sign-in of a user. The simulation estimates the impact this sign-in has on your policies and generates a simulation report. The report does not only list the applied conditional access policies but also classic policies if they exist.
Reference:
https://azure.microsoft.com/en-us/updates/azure-ad-conditional-access-what-if-tool-is-now-available

HOTSPOT -

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

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

You have the locations shown in the following table.

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

The tenant contains a named location that has the following configurations:

⇨ Name: Location1

⇨ Mark as trusted location: Enabled

IPv4 range: 10.10.0.0/16 -

▪

MFA has a trusted IP address range of 193.17.17.0/24.

⇨ Name: CAPolicy1

⇨ Assignments

- Users or workload identities: Group1
- Cloud apps or actions: All cloud apps

⇨ Conditions

- Locations: All trusted locations

⇨ Access controls

- Grant
- Grant access: Require multi-factor authentication
- Session: 0 controls selected

⇨ Enable policy: On

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

NOTE: Each correct selection is worth one point.

Hot Area:

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

Correct Answer:

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

Box 1: No -

10.10.0.150 is from a trusted location.

Note: The trusted IPs feature of Azure AD Multi-Factor Authentication bypasses multi-factor authentication prompts for users who sign in from a defined IP address range. You can set trusted IP ranges for your on-premises environments. When users are in one of these locations, there's

no Azure AD Multi-Factor
Authentication prompt. The trusted IPs feature requires Azure AD Premium P1 edition.

Box 2: No -
10.10.1.160 is from a trusted location

Box 3: Yes -
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings

HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant named contoso.com that has Email one-time passcode for guests set to Yes.

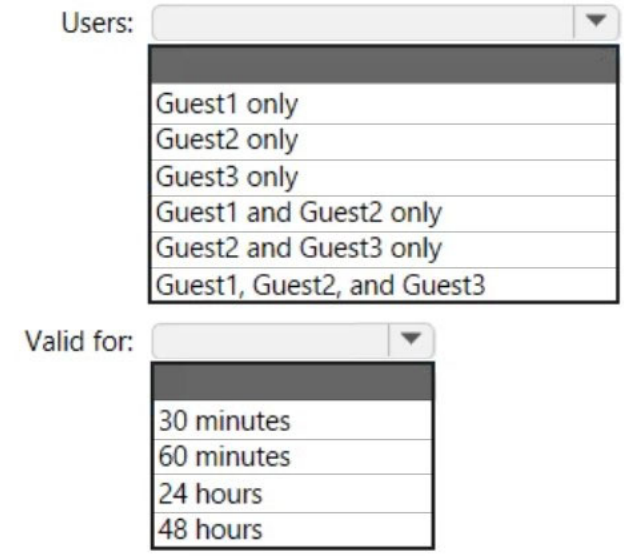
You invite the guest users shown in the following table.

Name	Email domain	Account type
Guest1	adatum.com	Azure AD account
Guest2	outlook.com	Microsoft account
Guest3	gmail.com	Personal Google account

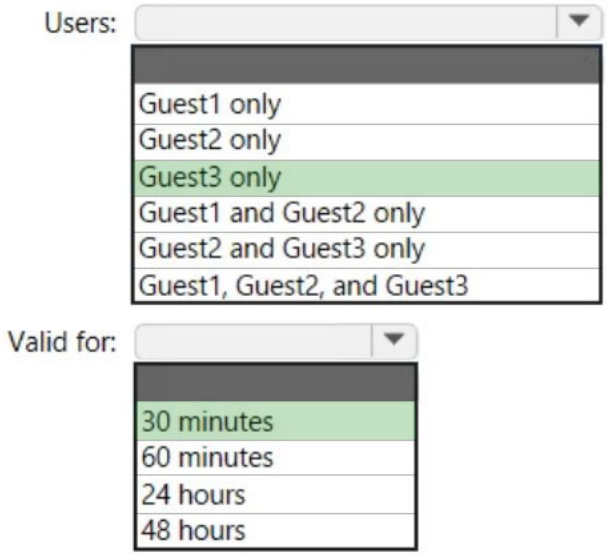
Which users will receive a one-time passcode, and how long will the passcode be valid? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Box 1: Guest3 only -

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

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

They don't have an Azure AD account

They don't have a Microsoft account

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

Box 2: 30 minutes -

One-time passcodes are valid for 30 minutes. After 30 minutes, that specific one-time passcode is no longer valid, and the user must request a new one. User sessions expire after 24 hours. After that time, the guest user receives a new passcode when they access the resource. Session expiration provides added security, especially when a guest user leaves their company or no longer needs access.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/one-time-passcode

Question #35 *Topic 2*

You have a Microsoft 365 tenant.

You currently allow email clients that use Basic authentication to connect to Microsoft Exchange Online.

You need to ensure that users can connect to Exchange only from email clients that use Modern authentication protocols.

What should you implement?

A. an OAuth policy in Microsoft Defender for Cloud Apps
B. a conditional access policy in Azure Active Directory (Azure AD)
C. a compliance policy in Microsoft Endpoint Manager
D. an application control profile in Microsoft Endpoint Manager

Correct Answer: *D*

Question #36 *Topic 2*

You have an Azure subscription that contains an Azure SQL database named db1.

You deploy an Azure App Service web app named App1 that provides product information to users that connect to App1 anonymously.

You need to provide App1 with access to db1. The solution must meet the following requirements:

• Credentials must only be available to App1.
• Administrative effort must be minimized.

Which type of credentials should you use?

A. a system-assigned managed identity
B. an Azure Active Directory (Azure AD) user account
C. a SQL Server account
D. a user-assigned managed identity

Correct Answer: *A*

Question #37 *Topic 2*

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

Name	Type
Role1	Azure Active Directory (Azure AD) role
Role2	Azure subscription role

You need to create a custom Azure subscription role named Role3 by using the Azure portal. Role3 will use the baseline permissions of an existing role.

Which roles can you clone to create Role3?

A. Role2 only

B. built-in Azure subscription roles only

C. built-in Azure subscription roles and Role2 only

D. built-in Azure subscription roles and built-in Azure AD roles only

E. Role1, Role2, built-in Azure subscription roles, and built-in Azure AD roles

Correct Answer: *C*

Question #38 *Topic 2*

You have a Microsoft 365 tenant.

All users have mobile phones and Windows 10 laptops.

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

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

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

A. Windows Hello for Business

B. an app password

C. security questions

D. email

Correct Answer: *B*

You have a Microsoft 365 tenant.

All users have mobile phones and Windows 10 laptops.

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

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

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

A. voice

B. Windows Hello for Business

C. email

D. security questions

Correct Answer: *A*

HOTSPOT
-

You have an Azure subscription that contains the following virtual machine:

• Name: V1
• Azure region: East US
• System-assigned managed identity: Disabled

You create the managed identities shown in the following table.

Name	Location
Managed1	East US
Managed2	East US
Managed3	West US

You perform the following actions:

• Assign Managed1 to V1.
• Create a resource group named RG1 in the West US region.

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
You can assign Managed2 to V1.	○	○
You can assign Managed3 to V1.	○	○
You can assign VM1 the Owner role for RG1.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
You can assign Managed2 to V1.	●	○
You can assign Managed3 to V1.	●	○
You can assign VM1 the Owner role for RG1.	○	●

HOTSPOT
-

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

Name	In resource group	Number of days to retain deleted key vaults	Purge protection
KeyVault1	RG1	15	Enabled
KeyVault2	RG1	10	Disabled

The subscription contains the users shown in the following table.

Name	Role
Admin1	Key Vault Administrator
Admin2	Key Vault Contributor
Admin3	Key Vault Certificates Officer
Admin4	Owner

On June 1, Admin4 performs the following actions:

• Deletes a certificate named Certificate1 from KeyVault1
• Deletes a secret named Secret1 from KeyVault2

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Admin1 can recover Secret1 on June 7.	○	○
Admin2 can purge Certificate1 on June 12.	○	○
Admin3 can purge Certificate1 on June 14.	○	○

Answer Area

	Statements	Yes	No
Correct Answer:	Admin1 can recover Secret1 on June 7.	○	○
	Admin2 can purge Certificate1 on June 12.	○	○
	Admin3 can purge Certificate1 on June 14.	○	○

Question #42 *Topic 2*

You have an Azure AD tenant.

You open the risk detections report.

Which risk detection type is classified as a user risk?

A. password spray

B. anonymous IP address

C. unfamiliar sign-in properties

D. Azure AD threat intelligence

Correct Answer: *D*

Question #43 *Topic 2*

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

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

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

What is a valid authentication method available to users?

A. a smartcard

B. a mobile app code

C. a mobile app notification

D. an email to an address outside your organization

Correct Answer: *B*

Question #44 *Topic 2*

You create a new Microsoft 365 E5 tenant.

You need to ensure that when users connect to the Microsoft 365 portal from an anonymous IP address, they are prompted to use multi-factor authentication (MFA).

What should you configure?

A. a sign-in risk policy

B. a user risk policy

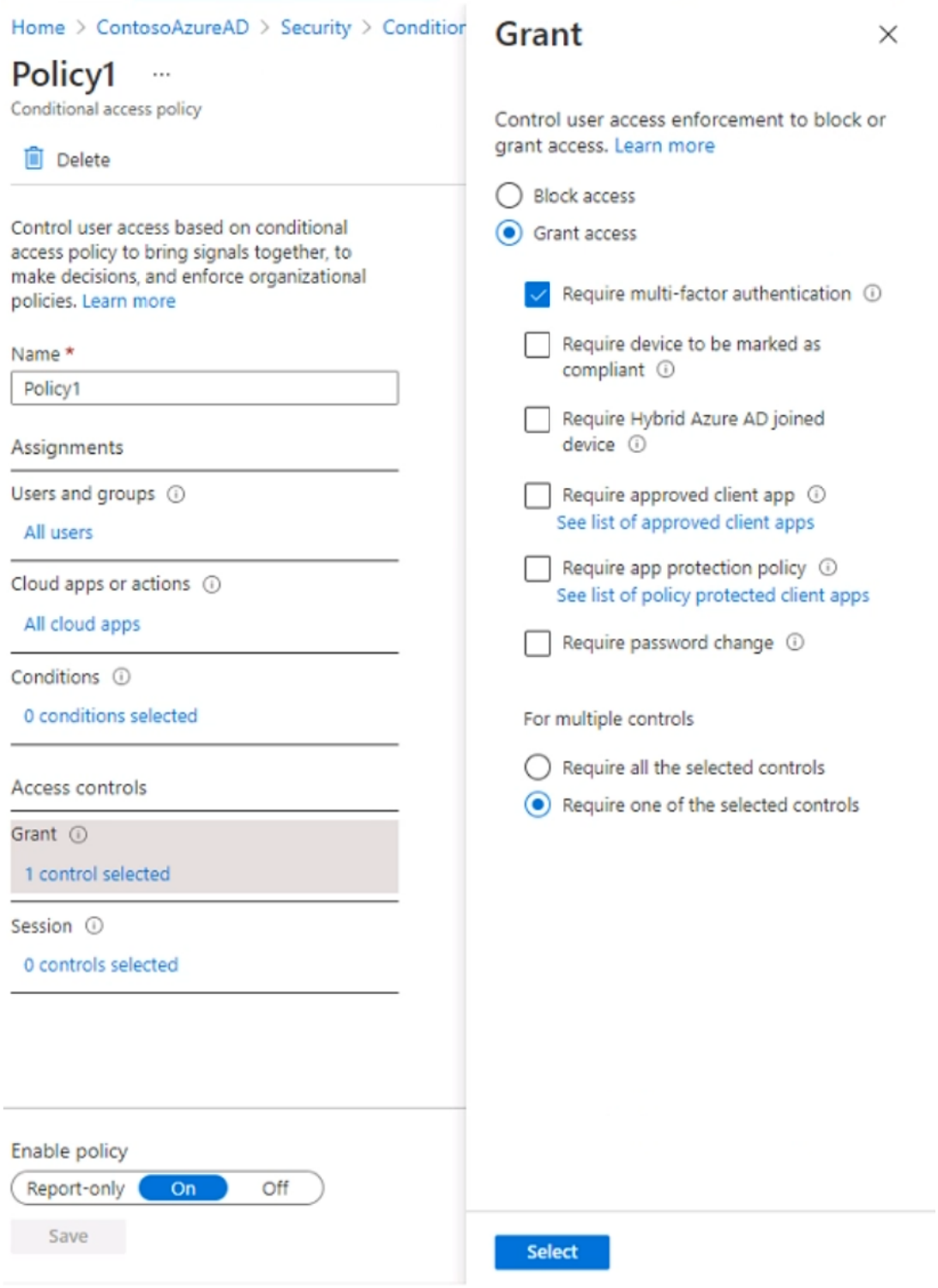
C. an MFA registration policy

Correct Answer: *A*

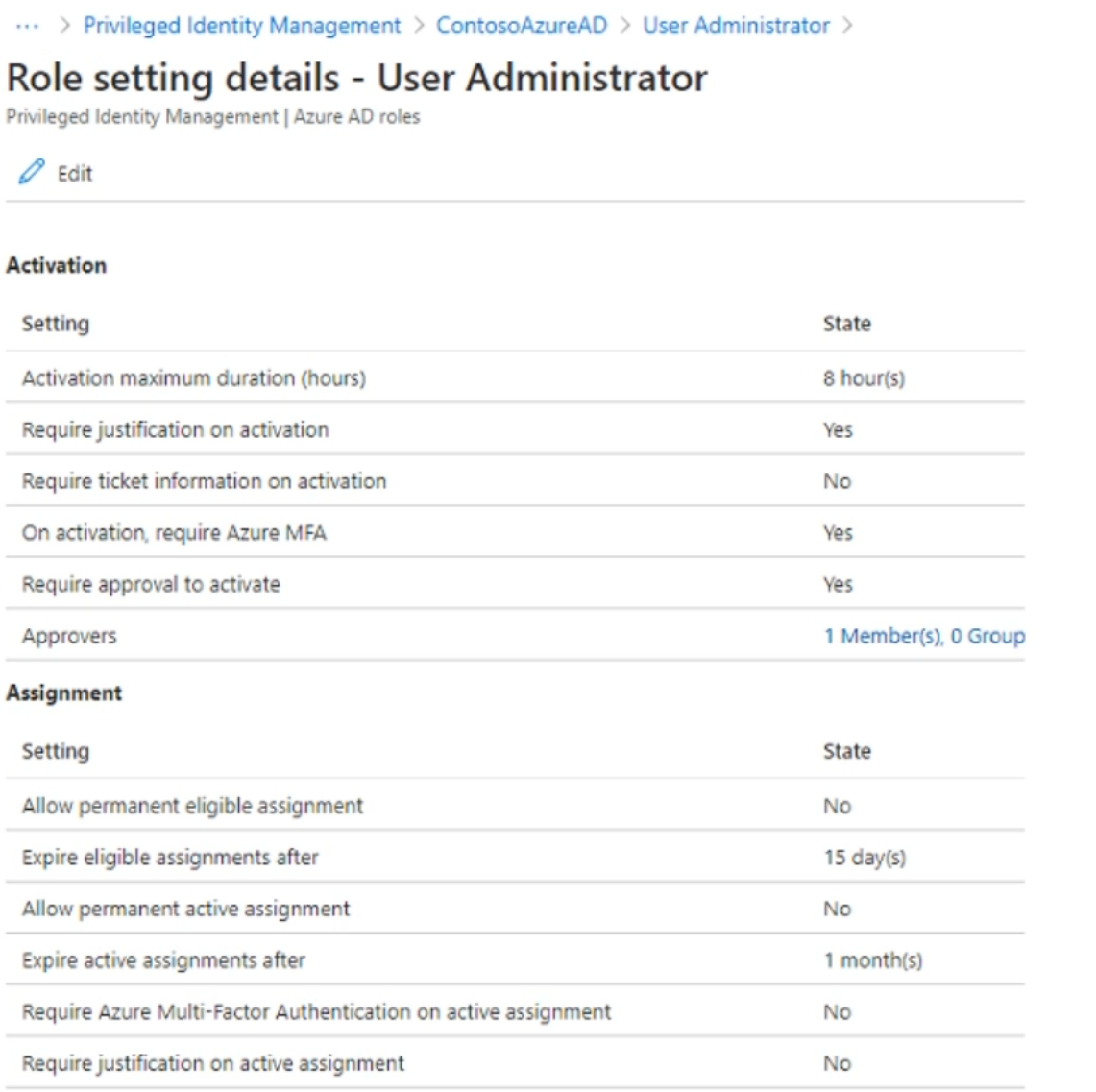
HOTSPOT
-

You have a Microsoft 365 tenant.

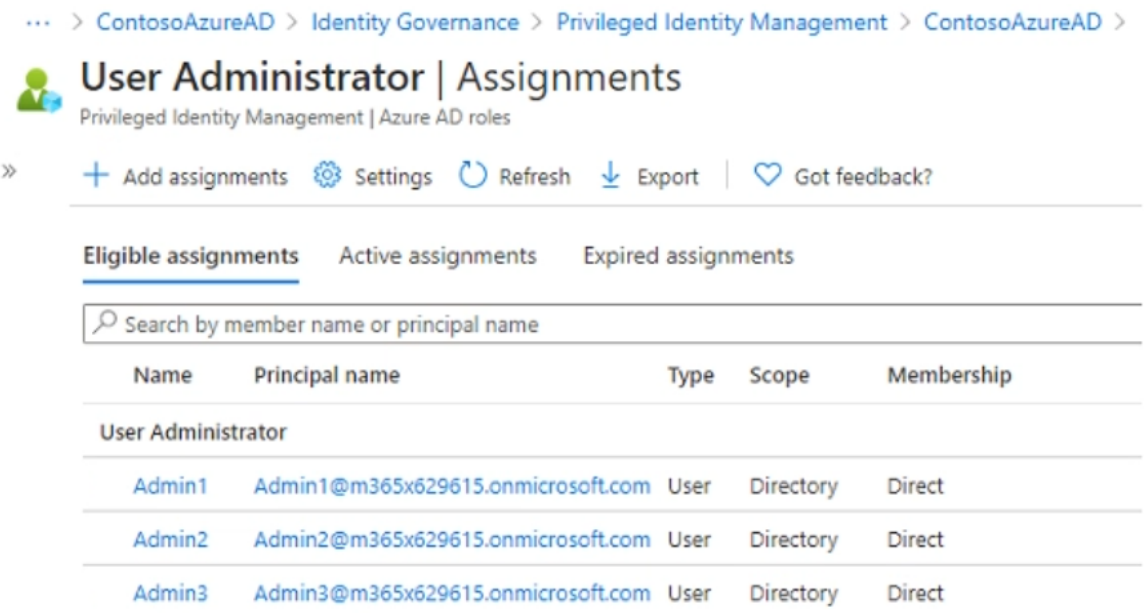
You configure a conditional access policy as shown in the Conditional Access policy exhibit. (Click the Conditional Access policy tab.)



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



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



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

NOTE: Each correct selection is worth one point.

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

Correct Answer:

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

HOTSPOT
-

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

Name	User risk level
User1	Low
User2	Medium
User3	High

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

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

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

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

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

NOTE: Each correct selection is worth one point.

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

Correct Answer:

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

Question #47 *Topic 2*

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

You need to meet the following requirements:

• Prevent User1 from being added as an owner of newly registered apps.
• Ensure that User1 can manage the application proxy settings.
• Ensure that User1 can register apps.
• Use the principle of least privilege.

Which role should you assign to User1?

A. Application developer
B. Cloud application administrator
C. Service support administrator
D. Application administrator

Correct Answer: *D*

Question #48 *Topic 2*

DRAG DROP
-

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

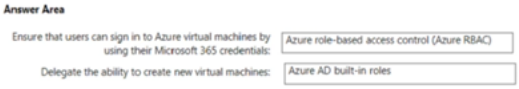
You need to meet the following requirements:

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

What should you use for each requirement? To answer, drag the appropriate features to the correct requirements. Each feature may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Correct Answer:



Question #49 *Topic 2*

You have a Microsoft 365 tenant.

All users have mobile phones and Windows 10 laptops.

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

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

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

A. a notification through the Microsoft Authenticator app

B. SMS

C. email

D. Windows Hello for Business

Correct Answer: *D*

HOTSPOT
-

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

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

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

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

NOTE: Each correct selection is worth one point.

Answer Area

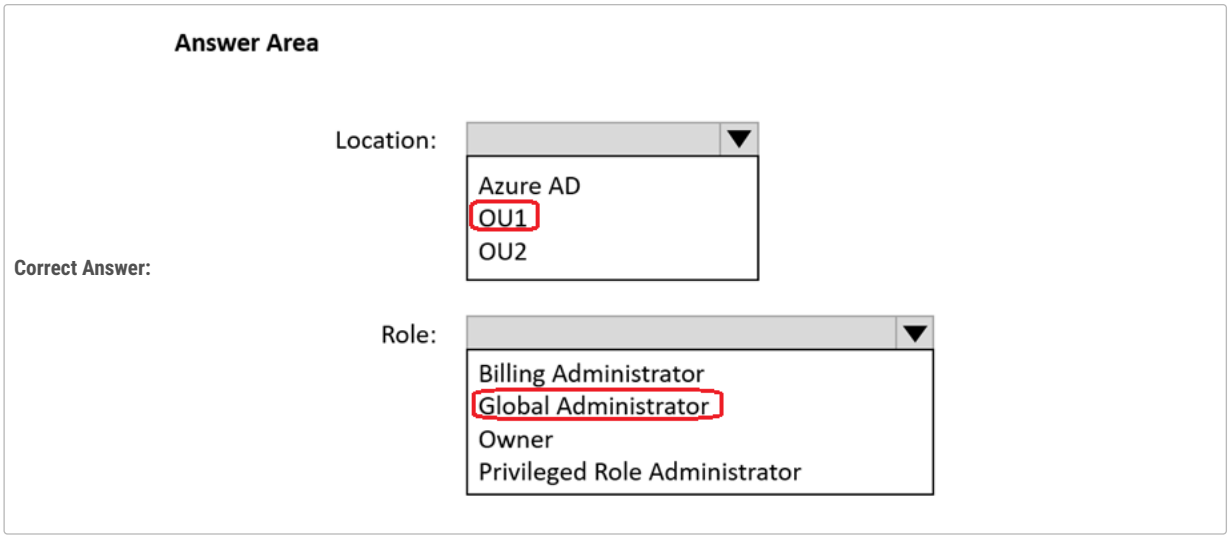
Location:

- Azure AD
- OU1
- OU2

Role:

- Billing Administrator
- Global Administrator
- Owner
- Privileged Role Administrator

Correct Answer:



Question #51 *Topic 2*

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

You need to ensure that users can request access to Site1. The solution must meet the following requirements:

- Automatically approve requests from users based on their group membership.
- Automatically remove the access after 30 days.

What should you do?

A. Create a Conditional Access policy.

B. Create an access package.

C. Configure Role settings in Azure AD Privileged Identity Management.

D. Create a Microsoft Defender for Cloud Apps access policy.

Correct Answer: *B*

HOTSPOT
-

You have an Azure subscription.

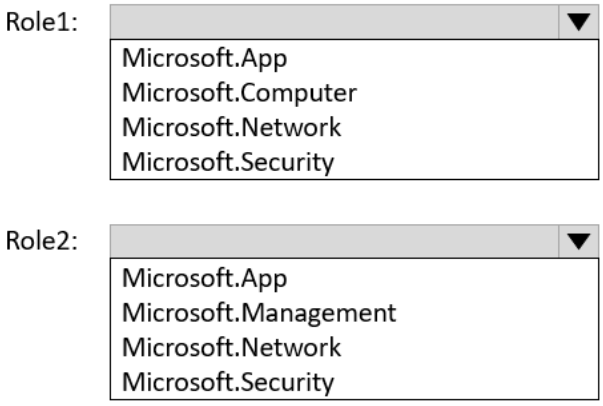
You need to create two custom roles named Role1 and Role2. The solution must meet the following requirements:

• Users that are assigned Role1 can manage application security groups.
• Users that are assigned Role2 can manage Azure Firewall.

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

NOTE: Each correct selection is worth one point.

Answer Area



Answer Area

Correct Answer:

Question #53 *Topic 2*

You have a Microsoft 365 tenant.

All users have mobile phones and Windows 10 laptops.

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

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

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

A. voice

B. an app password

C. security questions

D. a verification code from the Microsoft Authenticator app

Correct Answer: *D*

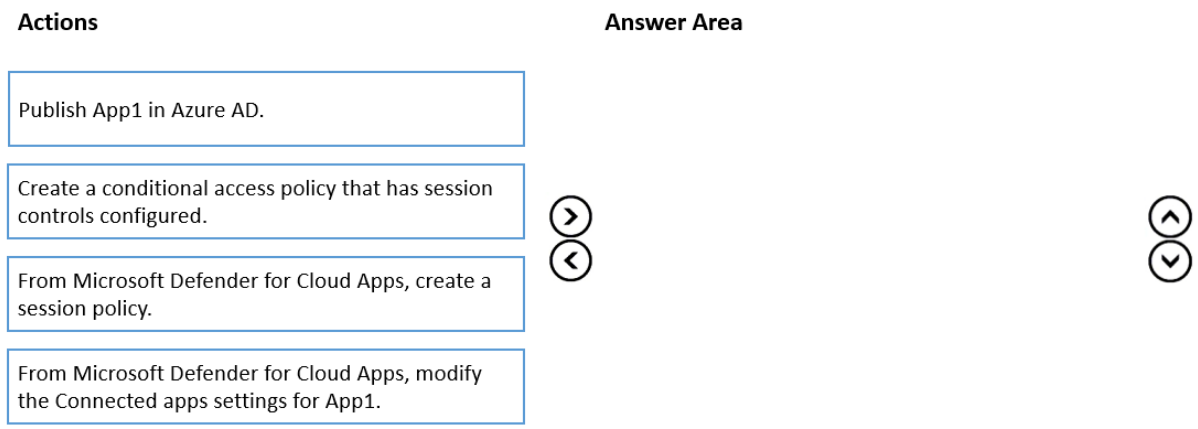
DRAG DROP
-

You have a Microsoft 365 E5 tenant.

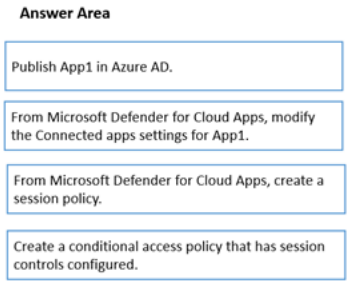
You purchase a cloud app named App1.

You need to enable real-time session-level monitoring of App1 by using Microsoft Defender for Cloud Apps.

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



Correct Answer:



Question #1 *Topic 3*

HOTSPOT -

You have a Microsoft 365 tenant and an Active Directory domain named adatum.com.

You deploy Azure AD Connect by using the Express Settings.

You need to configure self-service password reset (SSPR) to meet the following requirements:

- When users reset their password, they must be prompted to respond to a mobile app notification or answer three predefined security questions.
- Passwords must be synced between the tenant and the domain regardless of where the password was reset.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

From the Password reset blade in the Azure Active Directory admin center, configure:

- Authentication methods
- Notifications
- Properties
- Registration

From Azure AD Connect, enable:

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

Correct Answer:

Answer Area

From the Password reset blade in the Azure Active Directory admin center, configure:

- Authentication methods
- Notifications
- Properties
- Registration

From Azure AD Connect, enable:

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

Reference:

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

HOTSPOT -

You have a Microsoft 365 tenant.

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

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

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

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

Answer Area

Correct Answer:

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

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

Reference:

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

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

A. Application Insights in Azure Monitor

B. access reviews in Azure AD

C. Cloud App Discovery in Microsoft Cloud App Security

D. enterprise applications in Azure AD

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

HOTSPOT -

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

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

The Active Directory forest syncs to an Azure Active Directory (Azure AD) tenant. Multi-factor authentication (MFA) is enforced for Azure AD.

You need to ensure that you can publish App1 to Azure AD users.

What should you configure on Server4 and Firewall1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Service to install on Server4:
- Azure AD Application Proxy
- The Azure AD Password Protection DC agent
- The Azure AD Password Protection proxy service
- Web Application Proxy in Windows Server

Rule to configure on Firewall1:
- Allow incoming HTTPS connections from Azure AD to Server4.
- Allow incoming IPsec connections from Azure AD to Server4.
- Allow outbound HTTPS connections from Server4 to Azure AD.
- Allow outbound IPsec connections from Server4 to Azure AD.

Correct Answer:

Answer Area

Service to install on Server4:
- Azure AD Application Proxy
- The Azure AD Password Protection DC agent
- The Azure AD Password Protection proxy service
- Web Application Proxy in Windows Server

Rule to configure on Firewall1:
- Allow incoming HTTPS connections from Azure AD to Server4.
- Allow incoming IPsec connections from Azure AD to Server4.
- Allow outbound HTTPS connections from Server4 to Azure AD.
- Allow outbound IPsec connections from Server4 to Azure AD.

Reference:

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

HOTSPOT -

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

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

You purchase two cloud apps named App1 and App2. The global administrator registers App1 in Azure AD.

You need to identify who can assign users to App1, and who can register App2 in Azure AD.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Can assign users to App1:
- Admin1 only
- Admin3 only
- Admin1 and Admin3 only
- Admin1, Admin2, and Admin3 only
- Admin1, Admin2, Admin3, and User1

Can register App2 in Azure AD:
- Admin1 only
- Admin3 only
- Admin1 and Admin3 only
- Admin1, Admin2, and Admin3 only
- Admin1, Admin2, Admin3, and User1

Correct Answer:

Answer Area

Can assign users to App1:
- Admin1 only
- Admin3 only
- **Admin1 and Admin3 only**
- Admin1, Admin2, and Admin3 only
- Admin1, Admin2, Admin3, and User1

Can register App2 in Azure AD:
- Admin1 only
- Admin3 only
- Admin1 and Admin3 only
- Admin1, Admin2, and Admin3 only
- **Admin1, Admin2, Admin3, and User1**

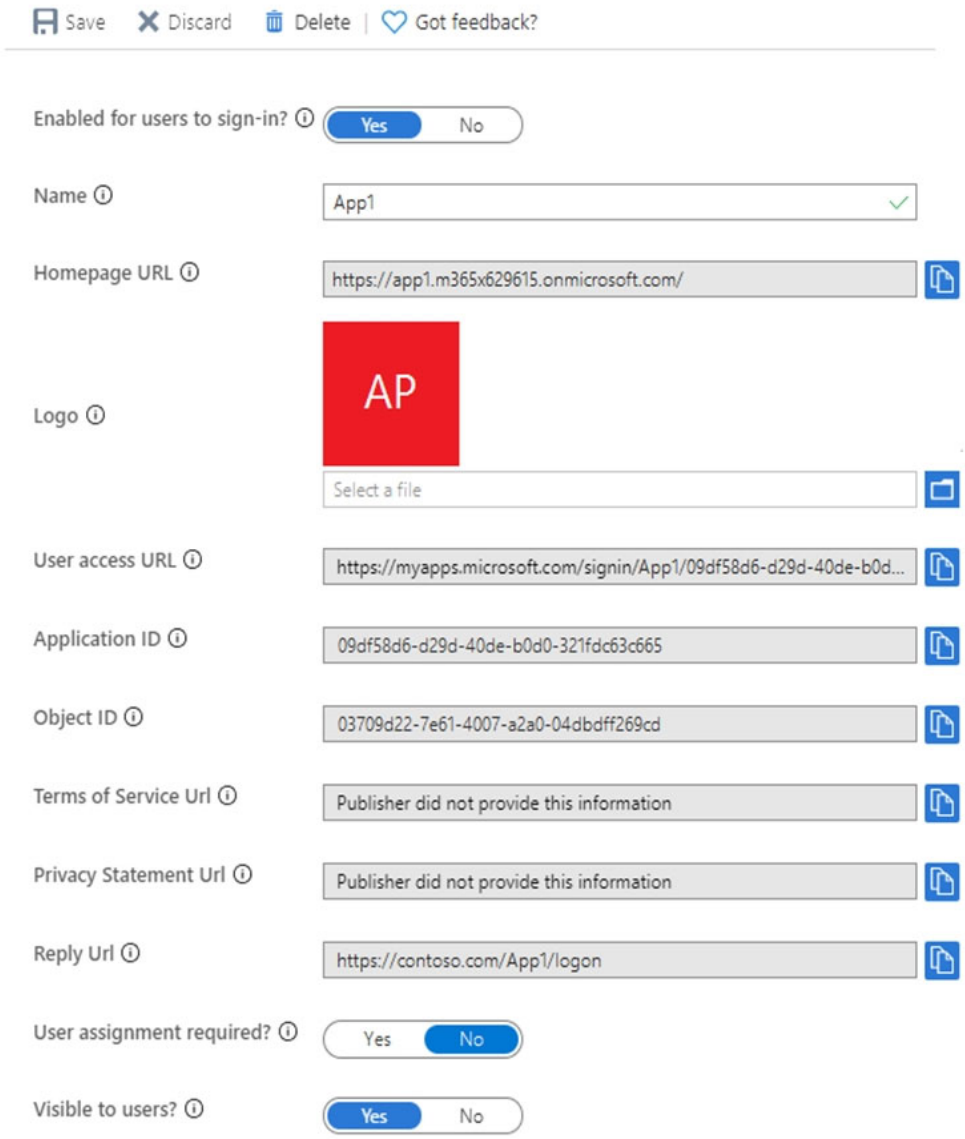
Reference:

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

HOTSPOT -

You have a custom cloud app named App1 that is registered in Azure Active Directory (Azure AD).

App1 is configured as shown in the following exhibit.



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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

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

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

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

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

Answer Area

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

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

Correct Answer:

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

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

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

Question #7 *Topic 3*

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

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

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

A. From Users and groups, add HRUsers.

B. From Single sign-on, configure a sign-on method.

C. From Properties, change User assignment required to No.

D. From Permissions, review the User consent permissions.

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

Question #8 *Topic 3*

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

A. Managed Application Contributor for Subscription1.

B. Application developer in Azure AD.

C. Cloud application administrator in Azure AD.

D. App Configuration Data Owner for Subscription1.

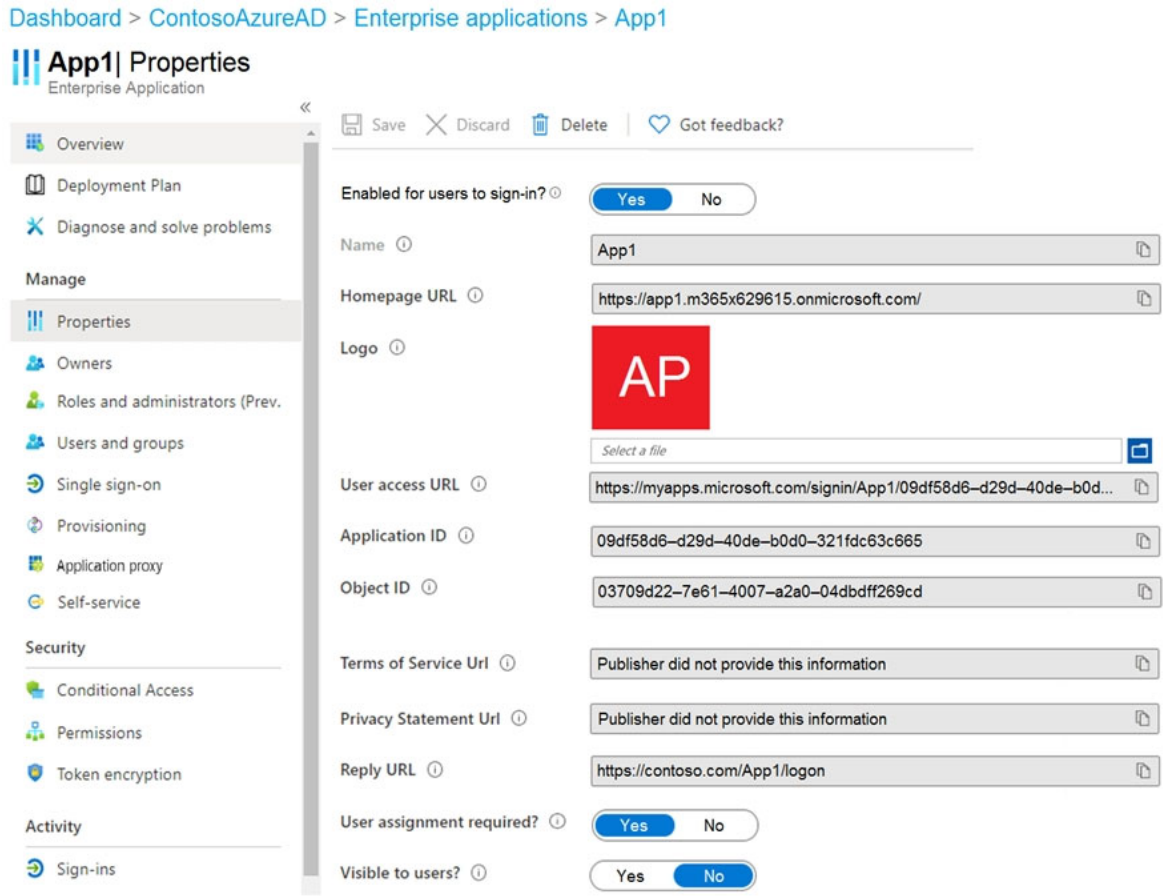
Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-app-roles

HOTSPOT -

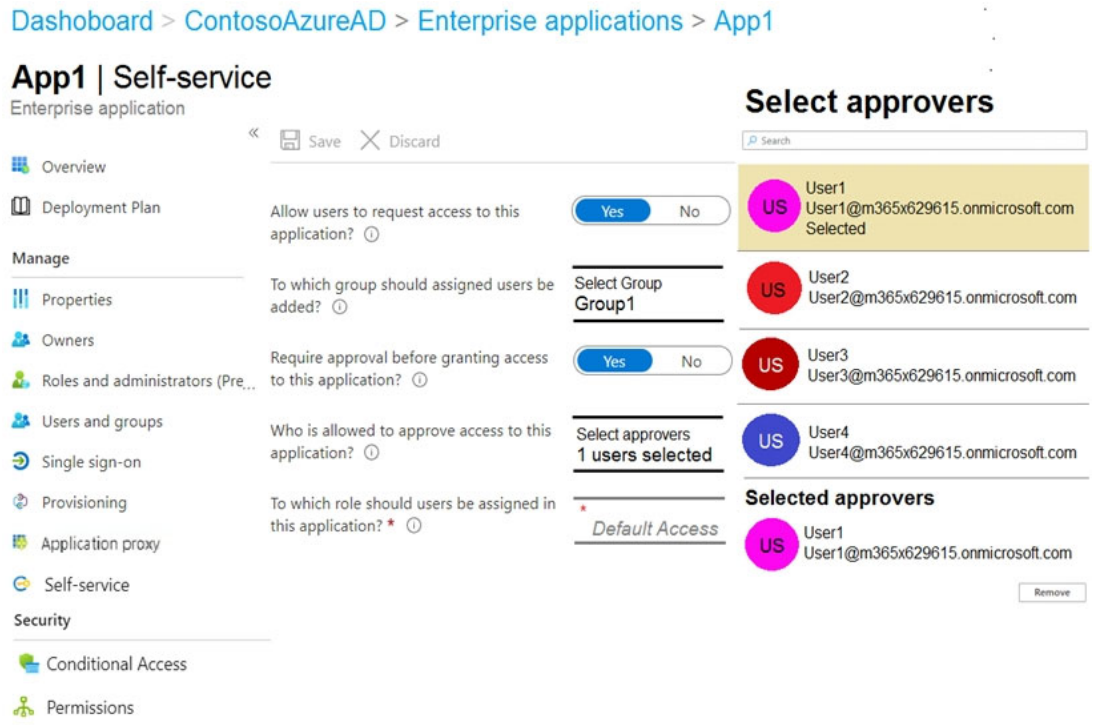
You have a Microsoft 365 tenant that contains a group named Group1 as shown in the Group1 exhibit. (Click the Group1 tab.)

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

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

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

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

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



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



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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

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

Answer Area

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

Reference:

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

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

A. Configure access reviews in Azure AD.

B. Enforce Azure AD Password Protection.

C. Configure self-service password reset (SSPR) for all users.

D. Implement multi-factor authentication (MFA) for all users.

Correct Answer: *D*
MFA and SSPR are both required. However, MFA is required first.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-remediate-unblock
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment

HOTSPOT -

Your company has a Microsoft 365 tenant.

All users have computers that run Windows 10 and are joined to the Azure Active Directory (Azure AD) tenant.

The company subscribes to a third-party cloud service named Service1. Service1 supports Azure AD authentication and authorization based on OAuth. Service1 is published to the Azure AD gallery.

You need to recommend a solution to ensure that the users can connect to Service1 without being prompted for authentication. The solution must ensure that the users can access Service1 only from Azure AD-joined computers. The solution must minimize administrative effort.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

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

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

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

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

Correct Answer:

Answer Area

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

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

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

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

Reference:

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

Question #12 *Topic 3*

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

A. Self-service

B. Provisioning

C. Application proxy

D. Roles and administrators

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

DRAG DROP -

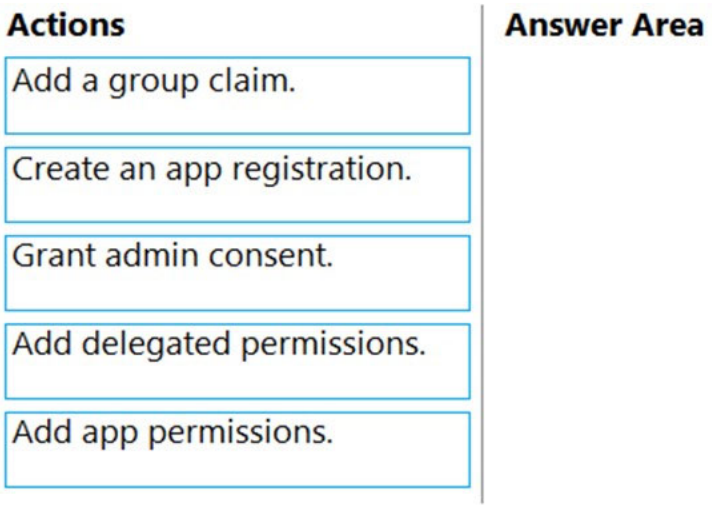
Your company has an Azure Active Directory (Azure AD) tenant named contoso.com.

The company is developing a web service named App1.

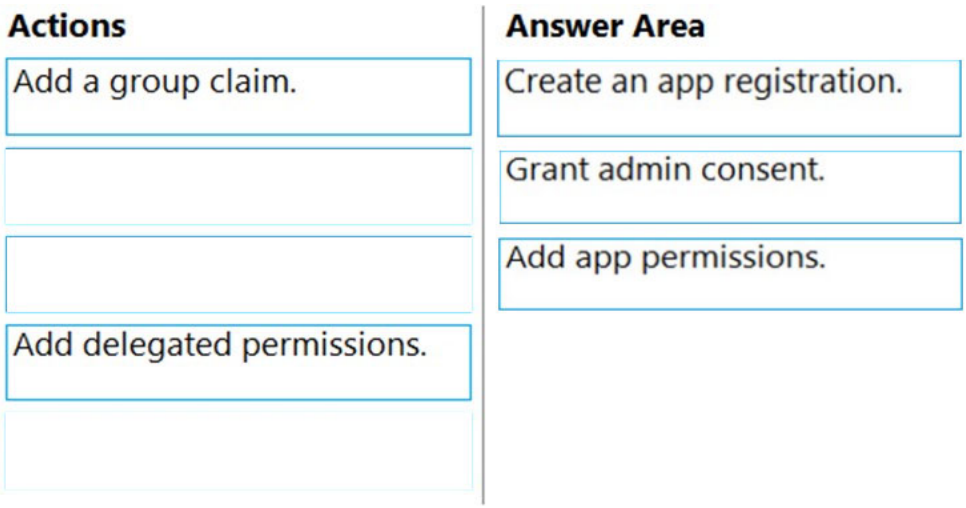
You need to ensure that App1 can use Microsoft Graph to read directory data in contoso.com.

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

Select and Place:



Correct Answer:



1. Create an app registration:

Your app must be registered with the Microsoft identity platform and be authorized by either a user or an administrator for access to the Microsoft Graph resources it needs.

2. Grant admin consent:

Higher-privileged permissions require administrator consent.

3. Add app permissions:

After the consents to permissions for your app, your app can acquire access tokens that represent the app's permission to access a resource in some capacity.

Encoded inside the access token is every permission that your app has been granted for that resource.

Reference:

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

Question #14 *Topic 3*

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

A. tags

B. collections

C. naming policies

D. dynamic groups

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

Question #15 *Topic 3*

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

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

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

A. Group1 only

B. Group2 only

C. Group3 only

D. Group1 and Group4

E. Group1 and Group3

Correct Answer: *E*
Using Azure Active Directory (Azure AD) with an Azure AD Premium license plan, you can use groups to assign access to a SaaS application that's integrated with Azure AD. For example, if you want to assign access for the marketing department to use five different SaaS applications, you can create an Office 365 or security group that contains the users in the marketing department, and then assign that group to these five SaaS applications that are needed by the marketing department.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-saasapps

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

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

The User settings for enterprise applications have the following configurations:

- Users can consent to apps accessing company data on their behalf: No
- Users can consent to apps accessing company data for the groups they own: No
- Users can request admin consent to apps they are unable to consent to: Yes

Who can review admin consent requests: Admin2, User2

▪

User1 attempts, to add an app that requires consent to access company data.

Which user can provide consent?

A. User1

B. User2

C. Admin1

D. Admin2

Correct Answer: *C*

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

Reference:

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

Question #17 *Topic 3*

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

A. Configure the Outlook 2013 clients to use modern authentication.

B. Upgrade the Outlook 2013 clients to Outlook 2016.

C. From the Exchange admin center, configure Organization Sharing.

D. Upgrade all the Outlook clients to Outlook 2019.

Correct Answer: *B*
From October 13, 2020 onward, only these versions of Office are supported for connecting to Microsoft 365 (and Office 365) services:
Microsoft 365 Apps for enterprise (previously named Office 365 ProPlus)
Microsoft 365 Apps for business (previously named Office 365 Business)
Office LTSC 2021, such as Office LTSC Professional Plus 2021
Office 2019, such as Office Professional Plus 2019
Office 2016, such as Office Standard 2016
Note:
Office 2019 and Office 2016 will be supported for connecting to Microsoft 365 (and Office 365) services until October 2023.
Note: Client software: To support tenant restrictions, client software must request tokens directly from Azure AD, so that the proxy infrastructure can intercept traffic. Browser-based Microsoft 365 applications currently support tenant restrictions, as do Office clients that use modern authentication (like OAuth 2.0).
Reference:
https://docs.microsoft.com/en-us/deployoffice/endofsupport/microsoft-365-services-connectivity https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/tenant-restrictions

Question #18 *Topic 3*

You have a Microsoft 365 E5 subscription.

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

What should you do first?

A. From the Microsoft Defender for Cloud Apps portal, select User monitoring.

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

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

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

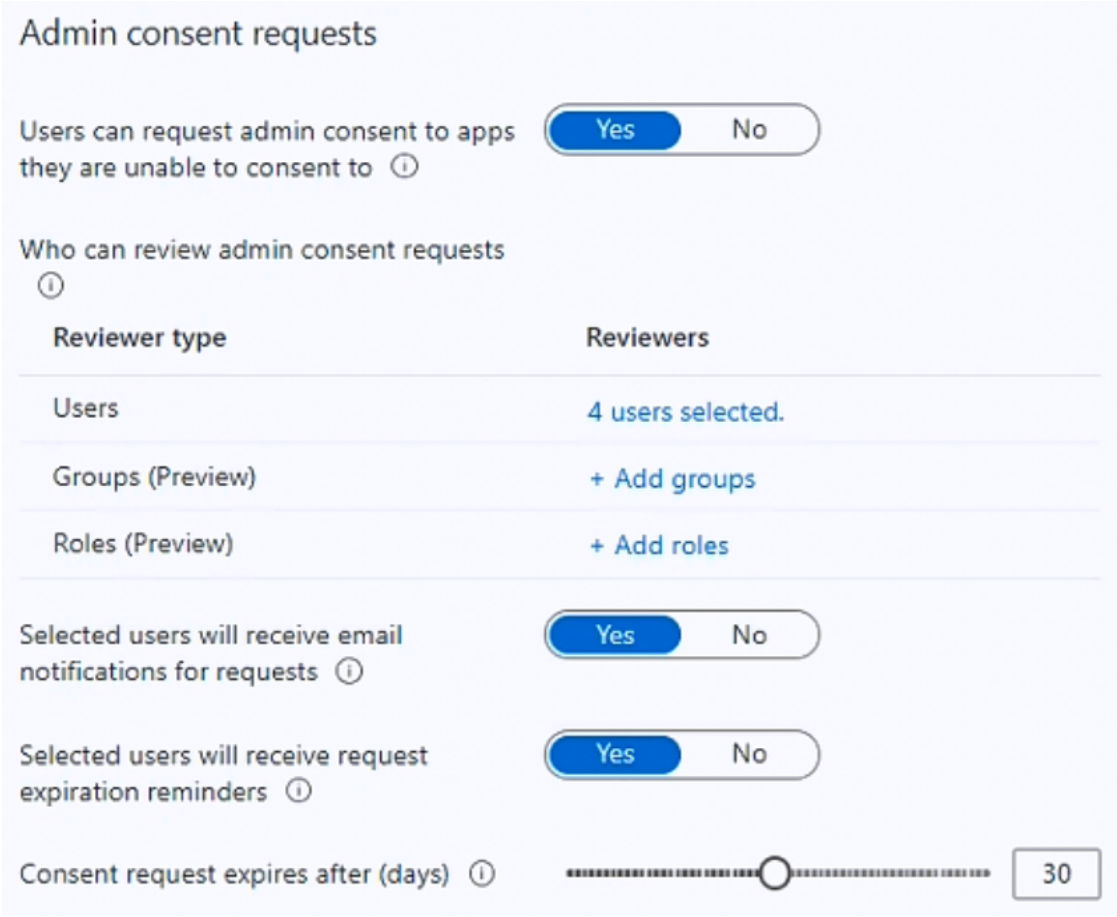
Correct Answer: *A*

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

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

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

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



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

Which users can review and approve the admin consent requests?

A. Admin1 only

B. Admin1, Admin2 and Admin3 only

C. Admin1, Admin2, and User1 only

D. Admin1 and Admin2 only

E. Admin1, Admin2, Admin3, and User1

Correct Answer: *D*

Question #20 *Topic 3*

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

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

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

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

Correct Answer: *B*

Question #21 *Topic 3*

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

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

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

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

Correct Answer: *D*

Question #22 *Topic 3*

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

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

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

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

Correct Answer: *A*

Question #23 *Topic 3*

You have a Microsoft 365 E5 subscription.

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

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

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

A. anomaly detection policy

B. OAuth app policy

C. access policy

D. activity policy

Correct Answer: *D*

Question #24 *Topic 3*

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

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

You have the app registrations shown in the following table.

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

A company policy prevents changes to user permissions.

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

A. User1

B. User2

C. User3

D. User4

Correct Answer: *B*

Question #25 *Topic 3*

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

User1 deletes the app registration of App1.

You need to restore the app registration.

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

A. 14

B. 30

C. 60

D. 180

Correct Answer: *B*

HOTSPOT
-

You have a Microsoft 365 tenant.

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

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

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

NOTE: Each correct selection is worth one point.

Answer Area

Tool to use:
- Azure AD Identity Protection
- Identity Governance
- Microsoft Defender for Cloud Apps
- Microsoft Endpoint Manager

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

Correct Answer:

Answer Area

Tool to use: Microsoft Defender for Cloud Apps

Policy type to create: OAuth app

Topic 4 - Question Set 4

Question #1 *Topic 4*

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

A. an access policy in Microsoft Cloud App Security.

B. Terms and conditions in Microsoft Endpoint Manager.

C. a conditional access policy in Azure AD

D. a compliance policy in Microsoft Endpoint Manager

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

Question #2 *Topic 4*

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

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

For which groups can you create an access review?

A. Group1 only

B. Group1 and Group4 only

C. Group1 and Group2 only

D. Group1, Group2, Group4, and Group5 only

E. Group1, Group2, Group3, Group4 and Group5

Correct Answer: *D*
You cannot create access reviews for device groups.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review

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

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

User1 is the owner of Group1.

You create an access review that has the following settings:

- Users to review: Members of a group
- Scope: Everyone
- Group: Group1
- Reviewers: Members (self)

Which users can perform access reviews for User3?

A. User1, User2, and User3

B. User3 only

C. User1 only

D. User1 and User2 only

Correct Answer: *B*

Reference:

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

HOTSPOT -

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

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

Role setting details - User Administrator

Privileged Identity Management | Azure AD roles

Edit

Activation

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

Assignment

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

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

- 8 hours
- 15 days
- 1 month

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

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

Correct Answer:

Answer Area

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

- 8 hours
- 15 days
- 1 month

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

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

Reference:

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

HOTSPOT -

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

User1 has the devices shown in the following table.

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

On November 5, 2020, you create and enforce terms of use in contoso.com that has the following settings:

- Name: Terms1
- Display name: Contoso terms of use
- Require users to expand the terms of use: On
- Require users to consent on every device: On
- Expire consents: On
- Expire starting on: December 10, 2020
- Frequency: Monthly

On November 15, 2020, User1 accepts Terms1 on Device3.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

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

Correct Answer:

Answer Area

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

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

Box 2: Yes because User1 has not yet accepted the terms on Device2. User1 will be prompted to register the device before the terms can be accepted.

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

Reference:

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

Question #6 *Topic 4*

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

A. Expire eligible assignments after from the Role settings details

B. Expire active assignments after from the Role settings details

C. Assignment type to Active

D. Assignment type to Eligible

Correct Answer: *D*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

Question #7 *Topic 4*

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

A. an access package that targets users outside your directory

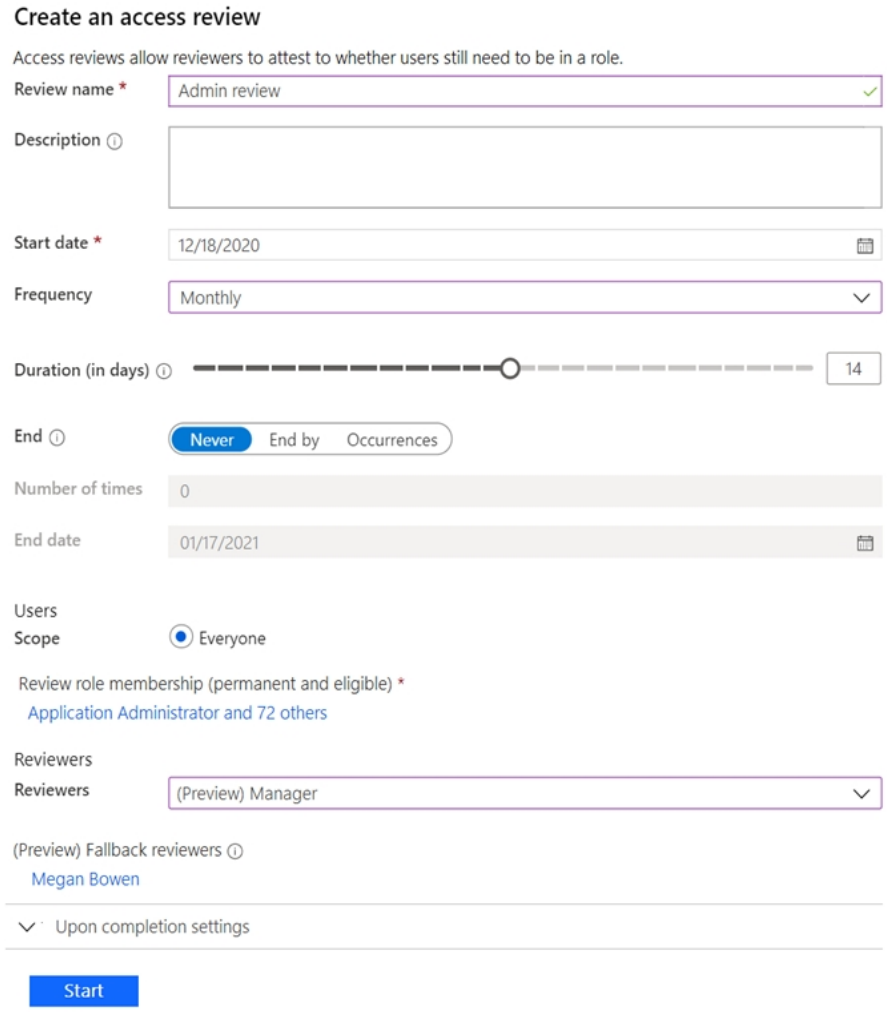
B. an access package that targets users in your directory

C. a group-based access review that targets guest users

D. an application-based access review that targets guest users

Correct Answer: *C*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview

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



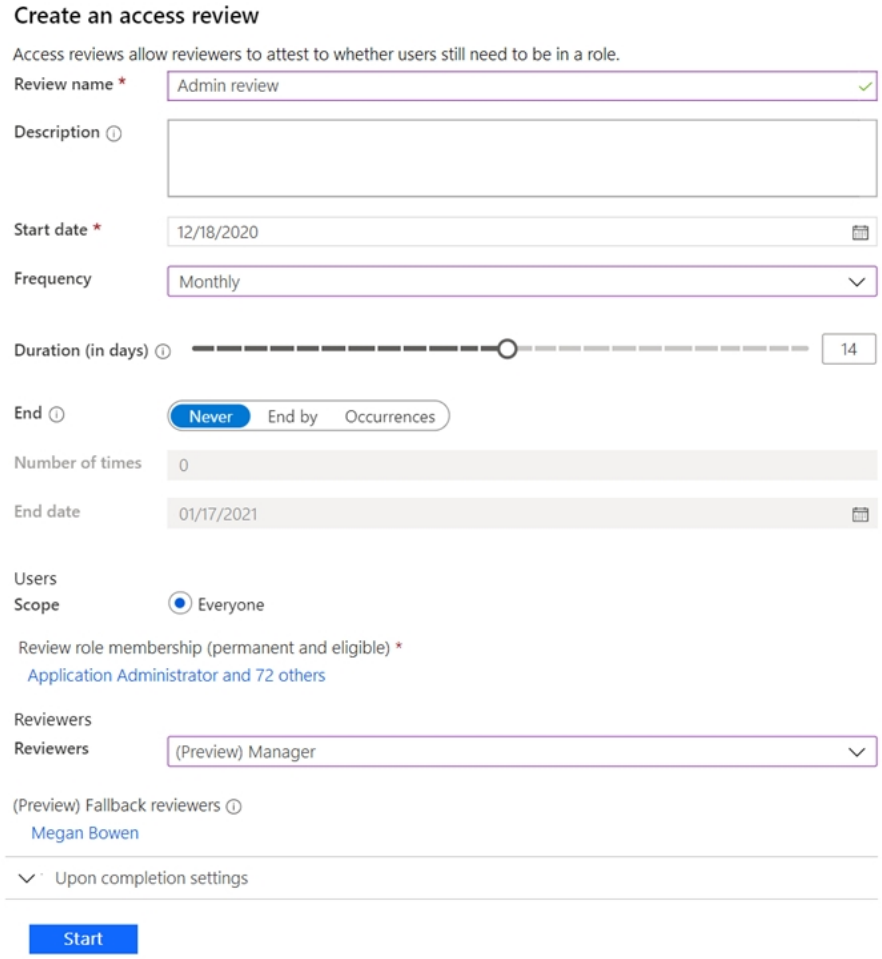
You discover that all access review requests are received by Megan Bowen.
You need to ensure that the manager of each department receives the access reviews of their respective department.
Solution: You create a separate access review for each role.
Does this meet the goal?

A. Yes

B. No

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

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



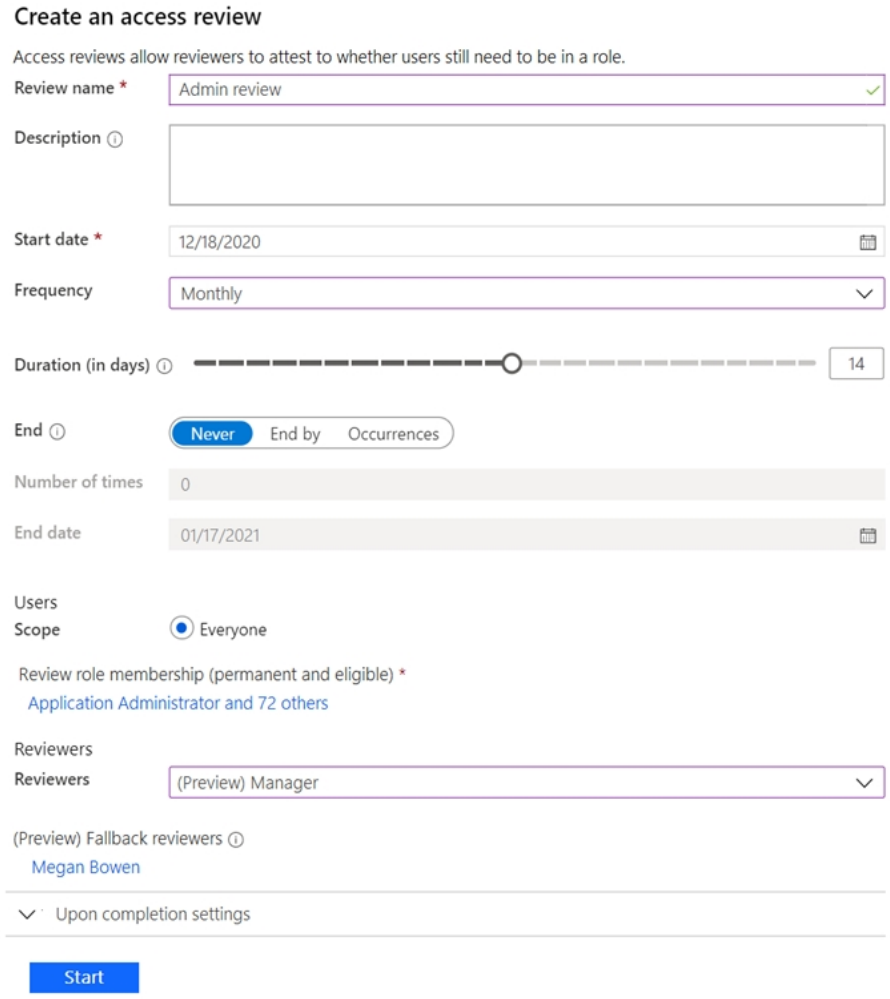
You discover that all access review requests are received by Megan Bowen.
You need to ensure that the manager of each department receives the access reviews of their respective department.
Solution: You modify the properties of the IT administrator user accounts.
Does this meet the goal?

A. Yes

B. No

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

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



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

A. Yes

B. No

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

Question #11 *Topic 4*

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

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

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

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

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

Correct Answer: *A*

Question #12 *Topic 4*

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

A. Access packages

B. Entitlement management settings

C. Terms of use

D. Access reviews settings

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

Question #13 *Topic 4*

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

A. 14 days

B. 30 days

C. 90 days

D. 365 days

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

Question #14 *Topic 4*

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

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

For which resources can you create an access review?

A. Group1, Role1, and Contributor only

B. Group1 only

C. Group1, App1, Contributor, and Role1

D. Role1 and Contributor only

Correct Answer: *C*
Access reviews require an Azure AD Premium P2 license.
Access reviews for Group1 and App1 can be configured in Azure AD Access Reviews.
Access reviews for the Contributor role and Role1 would need to be configured in Privileged Identity Management (PIM). PIM is included in Azure AD Premium
P2.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-start-security-review?toc=/azure/active-directory/governance/ toc.json https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview

Question #15 *Topic 4*

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

A. audit logs in CSV format

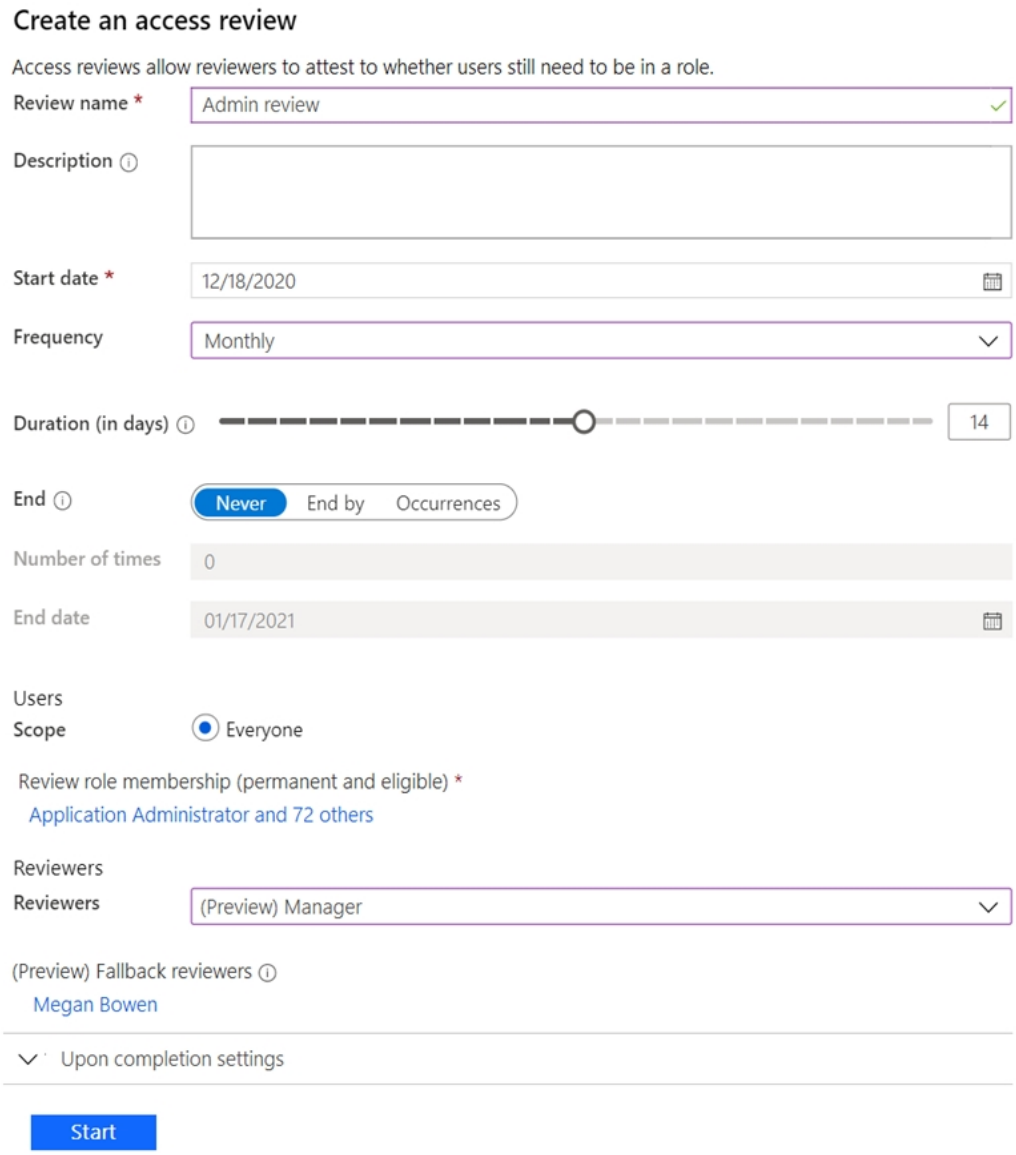
B. sign-ins in CSV format

C. audit logs in JSON format

D. sign-ins in JSON format

Correct Answer: *C*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-audit-logs

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



You discover that all access review requests are received by Megan Bowen.
You need to ensure that the manager of each department receives the access reviews of their respective department.
Solution: You add each manager as a fallback reviewer.
Does this meet the goal?

A. Yes

B. No

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

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

Name	Type
User1	User
Guest1	Guest
Identity1	Managed identity

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

A. User1, Guest1, and Identity1

B. User1 and Guest1 only

C. User1 only

D. User1 and Identity1 only

Correct Answer: *B*

Reference:

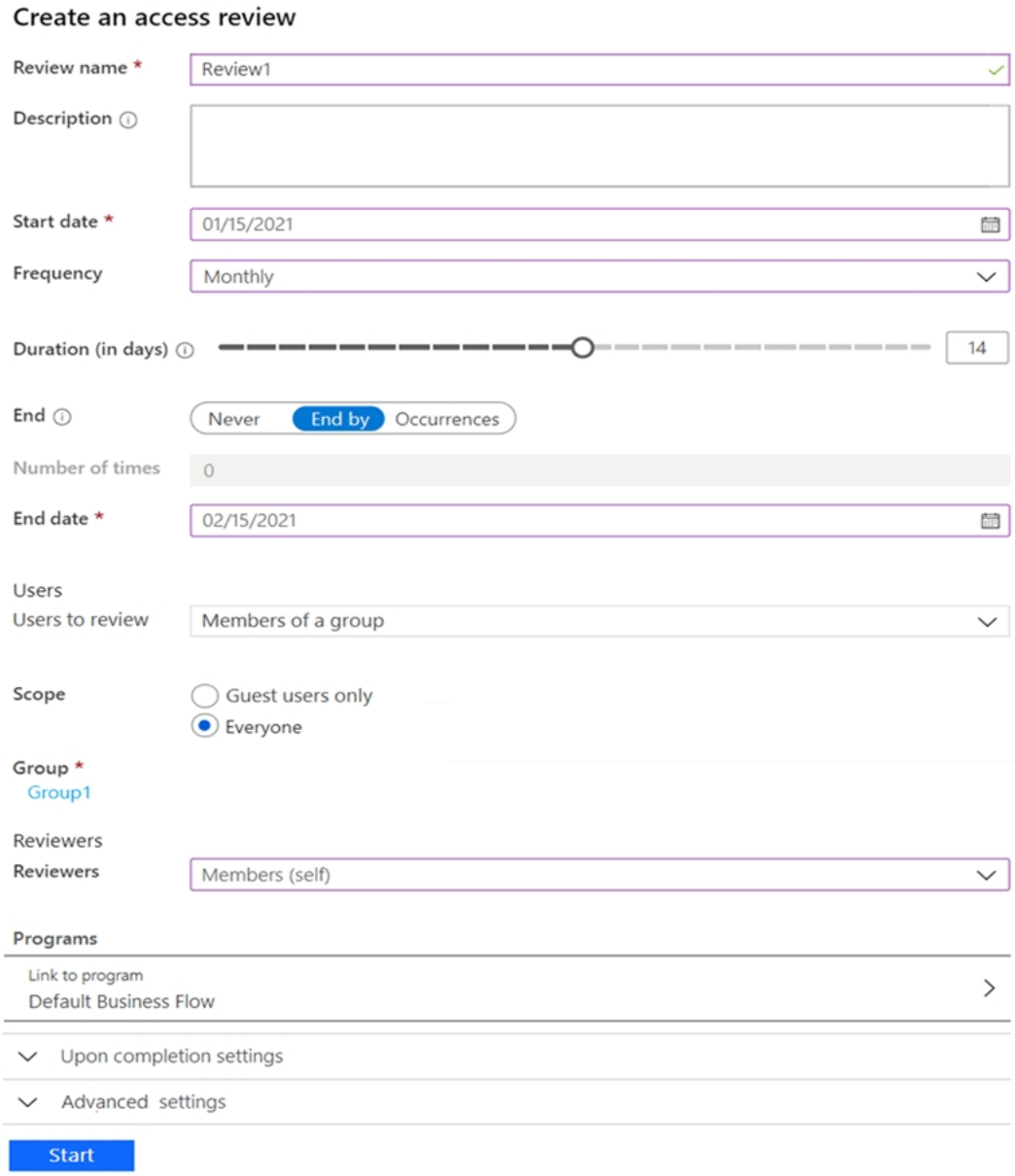
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-deployment-plan

HOTSPOT -

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

- Name: Group1
- Members: User1, User2
- Owner: User3

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



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

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

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

Correct Answer:

Answer Area

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

Reference:

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

HOTSPOT -

Your company has an Azure Active Directory (Azure AD) tenant named contoso.com. The company has a business partner named Fabrikam, Inc.

Fabrikam uses Azure AD and has two verified domain names of fabrikam.com and litwareinc.com. Both domain names are used for Fabrikam email addresses.

You plan to create an access package named package1 that will be accessible only to the users at Fabrikam.

You create a connected organization for Fabrikam.

You need to ensure that the package1 will be accessible only to users who have fabrikam.com email addresses.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

To allow access for users who have fabrikam.com email addresses, configure:

- An access package assignment in Identity Governance
- An access package policy in Identity Governance
- A conditional access policy in Azure AD
- The External collaboration settings in Azure AD

To block access for users who have litwareinc.com email addresses, configure:

- An access package assignment in Identity Governance
- An access package policy in Identity Governance
- A conditional access policy in Azure AD
- The External collaboration settings in Azure AD

Correct Answer:

Answer Area

To allow access for users who have fabrikam.com email addresses, configure:

- An access package assignment in Identity Governance
- **An access package policy in Identity Governance**
- A conditional access policy in Azure AD
- The External collaboration settings in Azure AD

To block access for users who have litwareinc.com email addresses, configure:

- An access package assignment in Identity Governance
- An access package policy in Identity Governance
- A conditional access policy in Azure AD
- **The External collaboration settings in Azure AD**

Reference:

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

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

Question #20 *Topic 4*

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

A. Add a Microsoft Sentinel data connector.

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

C. Create a Microsoft Sentinel playbook.

D. Modify the Diagnostics settings in Azure AD.

Correct Answer: *A*
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-ad-identity-protection

Question #21 *Topic 4*

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

A. Yes

B. No

Correct Answer: *B*

Question #22 *Topic 4*

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

A. Yes

B. No

Correct Answer: *A*

Question #23 *Topic 4*

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

A. Yes

B. No

Correct Answer: *B*

Question #24 *Topic 4*

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

A. Run the Set-AzureADTenantDetail cmdlet.

B. Create an Azure AD workbook.

C. Modify the Diagnostics settings for Azure AD.

D. Run the Get-AzureADAuditDirectoryLogs cmdlet.

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

HOTSPOT -

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

Name	Role
User1	None
User2	Privileged authentication administrator
User3	Global administrator

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

Edit

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

Assignment

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

User1 is eligible for the Global administrator role.

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

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

Correct Answer:

Box 1: Yes -

MFA is required on activation -

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

Box 3: No -
The Privileged Authentication Administrator can set or reset any authentication method for any user, including Global Administrators.
The Privileged Role Administrator can manage role assignments, including the Global Administrator role, in Azure Active Directory, as well as within Azure AD
Privileged Identity Management. In addition, this role allows management of all aspects of Privileged Identity Management and administrative units.

Question #26 *Topic 4*

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

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

A. Configure an app registration.

B. Create an Administrative unit.

C. Create an access package.

D. Create a catalog.

Correct Answer: *C*

Question #27 *Topic 4*

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

A. Yes

B. No

Correct Answer: *B*

HOTSPOT -

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

The tenant contains the groups shown in the following table.

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

The tenant contains the users shown in the following table.

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

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

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

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

Correct Answer:

Answer Area

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

Box 1: No -
User1 is member of Group1. Group1 is in the cloud. Group1 is member of Group3. Group3 is in the cloud.
The access review applies to Group3, but not to Group1. The access review is setup to remove access if reviewers don't respond.

Box 2: Yes -
User2 is member of Group2. Group1 is in an Active Directory domain.
The access review applies to Group2.

Box 3: No -
User3 is member of Group3, not of Group2.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview

Question #29 *Topic 4*

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

A. a Conditional Access policy

B. a compliance policy

C. a guest access review

D. an access review for application access

Correct Answer: *D*
Access to groups and applications for employees and guests changes over time. To reduce the risk associated with stale access assignments, administrators can use Azure Active Directory (Azure AD) to create access reviews for group members or application access.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review

HOTSPOT -

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

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

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

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

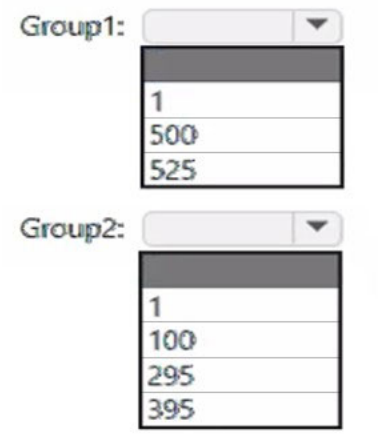
You create an access review for Group2 as shown in the following table.

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

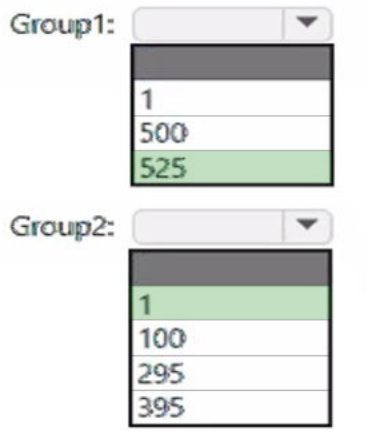
What is the minimum member of Azure Active Directory Premium P2 licenses required for each group? To answer, select the appropriate, options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Box 1: 525 -

For Group1:

Review scope: All Users, Reviewers: Users review own access

Note: How many licenses must you have?

Your directory needs at least as many Azure AD Premium P2 licenses as the number of employees who will be performing the following tasks:
Member users who are assigned as reviewers
Member users who perform a self-review
Member users as group owners who perform an access review
Member users as application owners who perform an access review
For guest users, licensing needs will depend on the licensing model you're using. However, the below guest users' activities are considered Azure AD Premium
P2 usage:
Guest users who are assigned as reviewers
Guest users who perform a self-review
Guest users as group owners who perform an access review
Guest users as application owners who perform an access review

Box 2: 1 -
For Group2:
Review scope: Guest users only. Reviewers: Group Owner.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview#license-requirements

HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains a group named All Company and has the following Identity Governance settings:

- Block external users from signing in to this directory: Yes
- Remove external user. Yes
- Number of days before removing external user from this directory: 30

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

- Resource rales

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

- Lifecycle

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

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

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

On March 2, 2022, you assign the Reports reader role to Guest1.

On April 1, 2022, you invite a guest user named Guest3 to contoso.com.

On April 4, 2022, you add Guest3 to the All Company group.

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

NOTE: Each correct selection is worth one point.

Hot Area:

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

Correct Answer:

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

Box 1: No -

On March 2, 2022, you assign the Reports reader role to Guest1.

On April 1 the access package assignment expires. After another 30 days, well before May 5, the guest user account is removed.

Box 2: No -

On April 1 the access package assignment expires. After another 30 days, well before May 5, the guest user account is removed.

Box 3: Yes -

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

Question #32 *Topic 4*

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

A. sign-in logs

B. the Usage and Insights report

C. provisioning logs

D. audit logs

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

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

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

User1 is the owner of Group1.

You create an access review that has the following settings:

- What to review: Teams + Groups
- Scope: All users
- Group: Group1
- Reviewers: Users review their own access

Which users can perform access reviews for User3?

A. User1 only

B. User3 only

C. User1 and User2 only

D. User1, User2, and User3

Correct Answer: *A*

Note:

If you set Select reviewers to Users review their own access or Managers of users, B2B direct connect users and Teams won't be able to review their own access in your tenant. The owner of the Team under review will get an email that asks the owner to review the B2B direct connect user and Teams.

Reference:

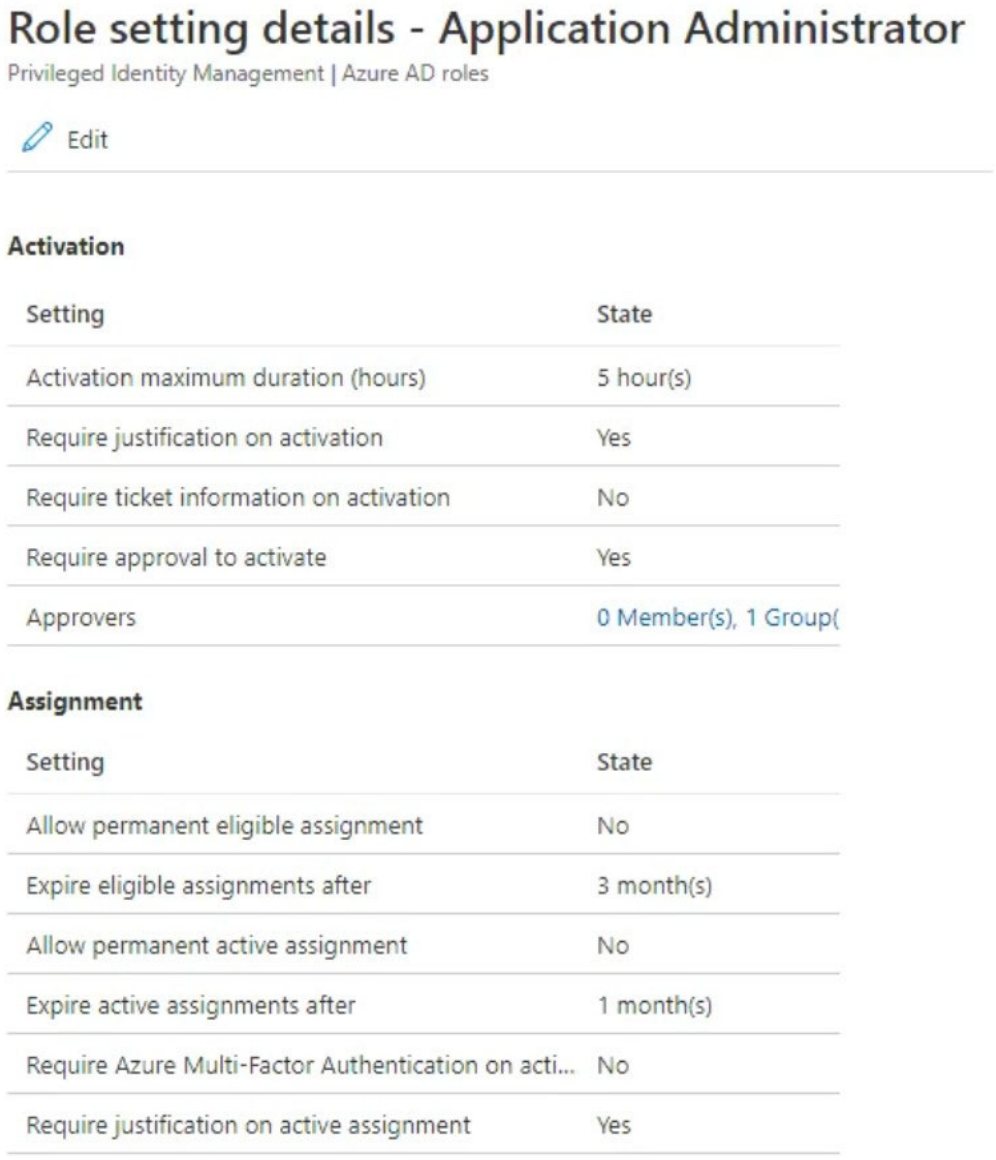
https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review

HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant that contains three users named User1, User2, and User3.

You create a group named Group1. You add User2 and User3 to Group1.

You configure a role in Azure AD Privileged Identity Management (PIM) as shown in the Application Administrator exhibit. (Click the Application Administrator tab.)



Role setting details - Application Administrator

Privileged Identity Management | Azure AD roles

Edit

Activation

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

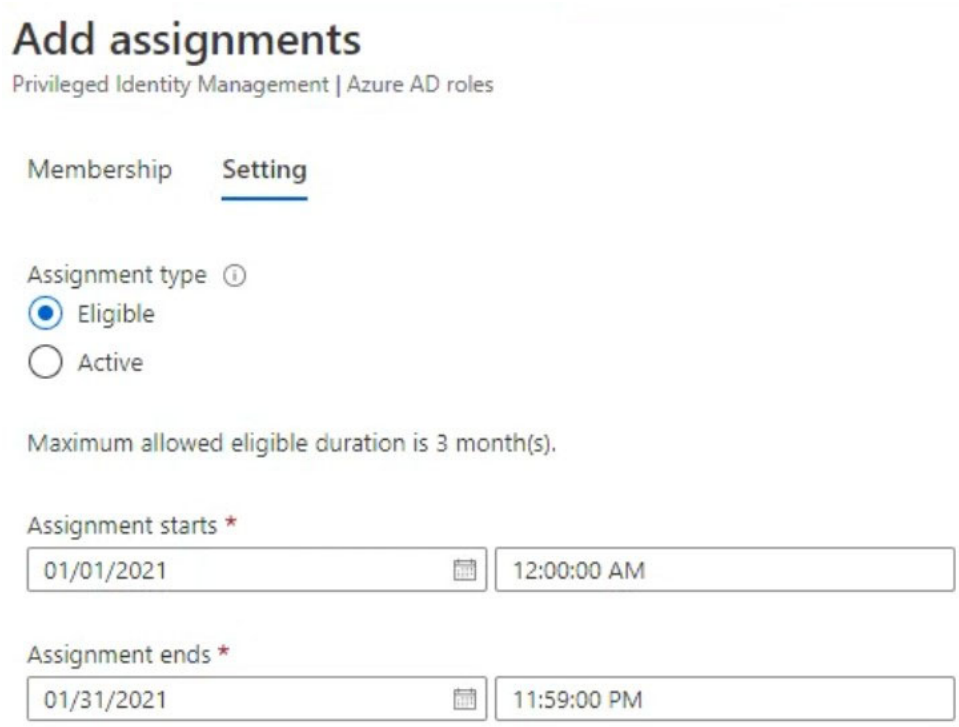
Assignment

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

Group1 is configured as the approver for the Application administrator role.

You configure User2 to be eligible for the Application administrator role.

For User1 you add an assignment to the Application administrator role as shown in the Assignment exhibit. (Click the Assignment tab.)



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

NOTE: Each correct selection is worth one point.

Hot Area:

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

Correct Answer:

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

Box 1: No -

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

However, here the Application Administrator role requires approval.

Box 2: No -

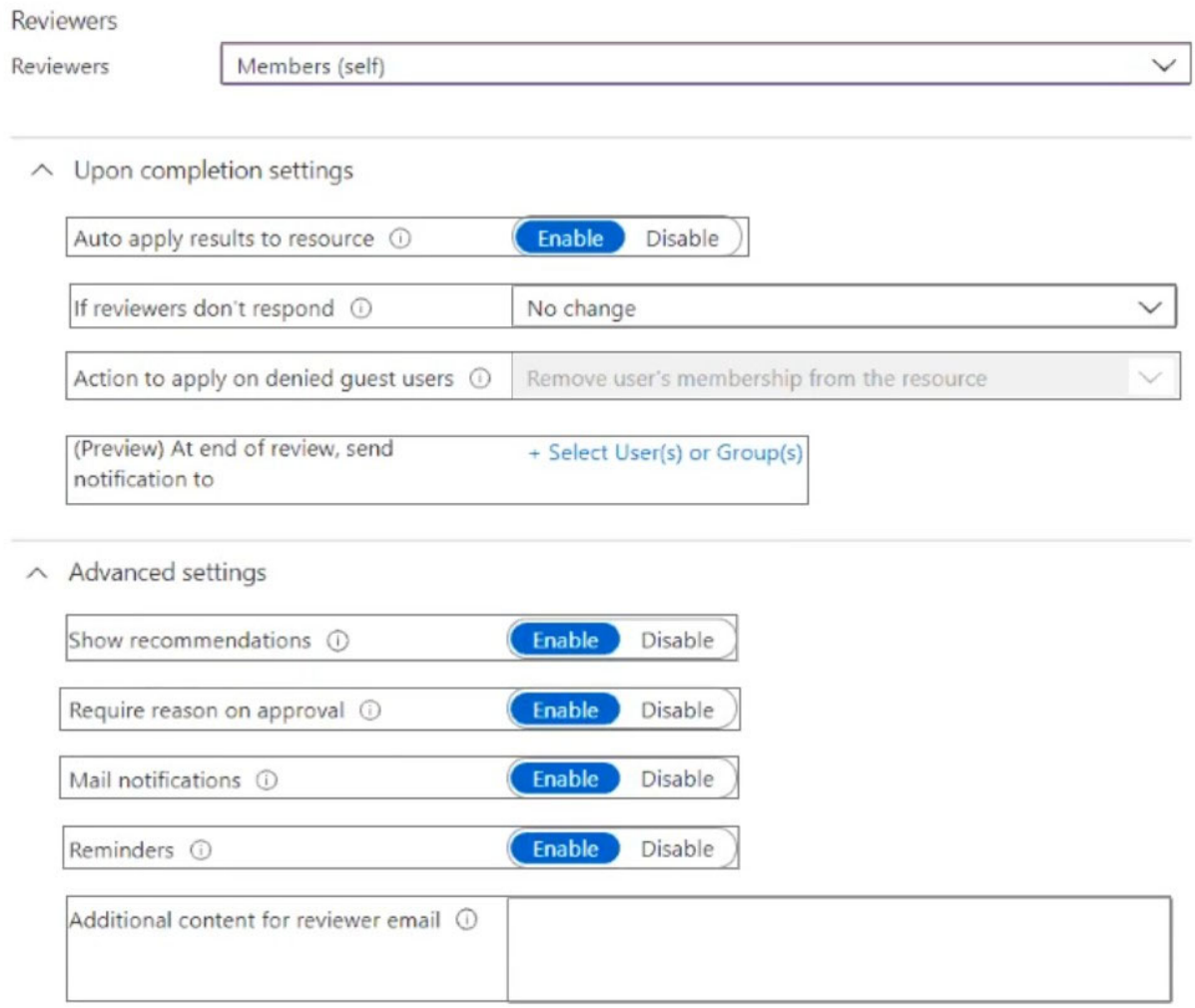
User2 is also member of Group1, and Group1 is configured as the approver for the Application administrator role.

Box 3: Yes -

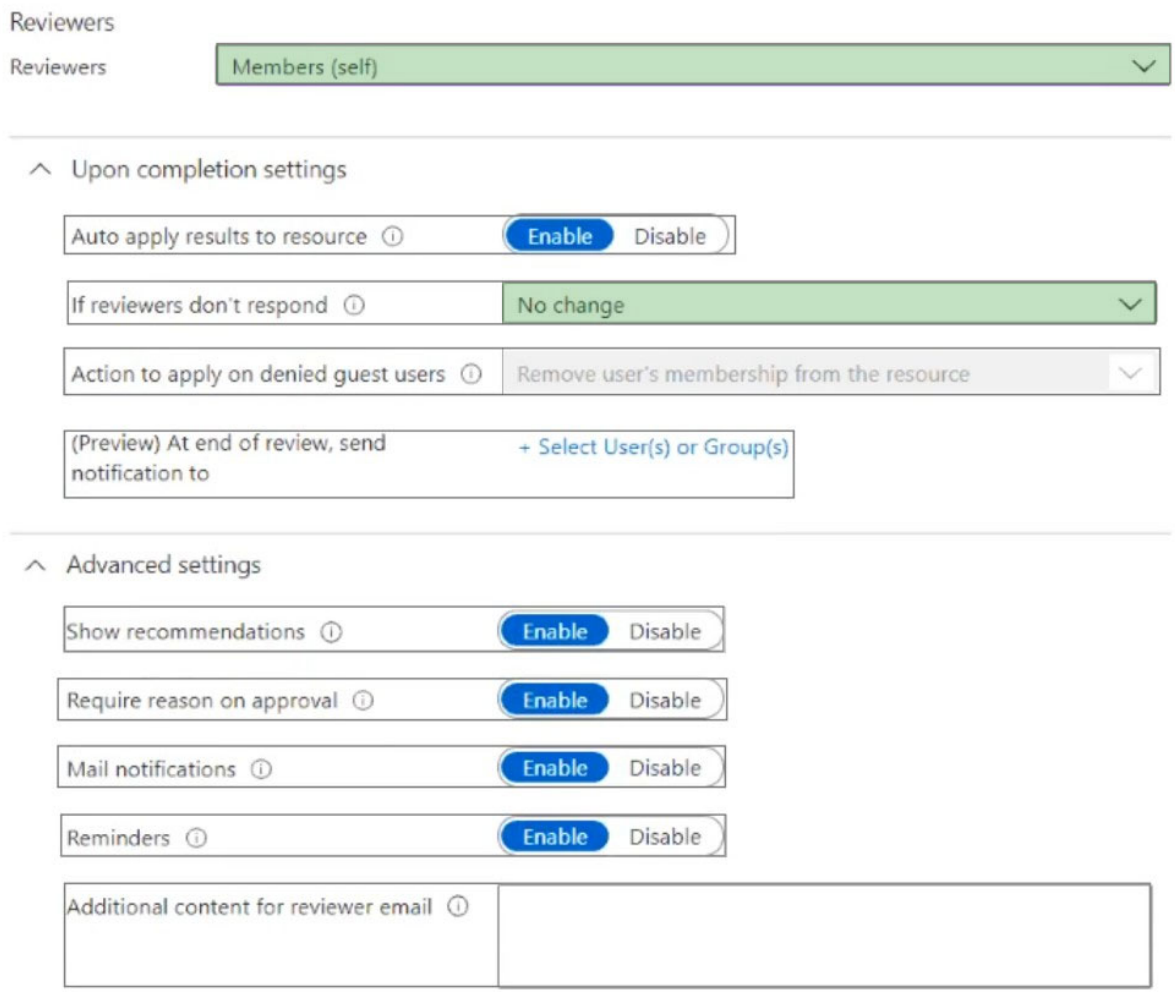
User1 is eligible from 1/1/2021 to 1/31/2021.

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

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



Correct Answer:



Box 1: Reviewers, Members (self)

Reviewers for guest users can be:

Specified reviewers: Certain users within your organization

Group owners: Office 365 Group owners that also includes Teams

Self-review: Guest users can review access on their own

Box 2: If reviewers don't respond, No Change

If reviewers don't respond (within the configured review period):

No change: Leave user's access unchanged

Remove access: Remove user's access

Approve access: Approve user's access

Take recommendations: Take the system's recommendation on denying or approving the user's continued access

Reference:

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

HOTSPOT
-

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

An administrator deletes User1.

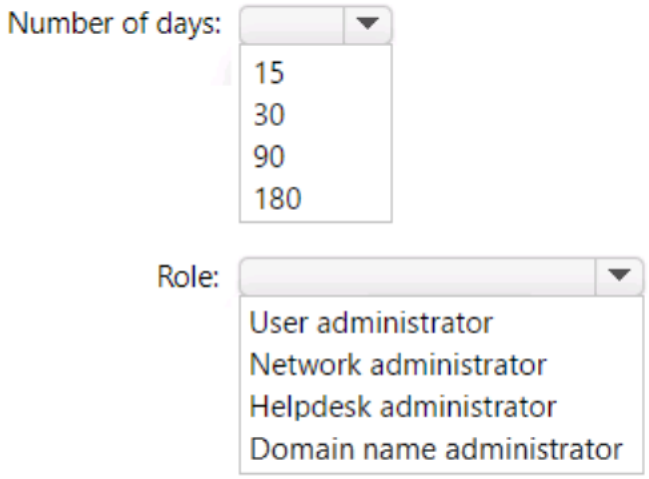
You need to identify the following:

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

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

NOTE: Each correct selection is worth one point.

Answer Area



Correct Answer:

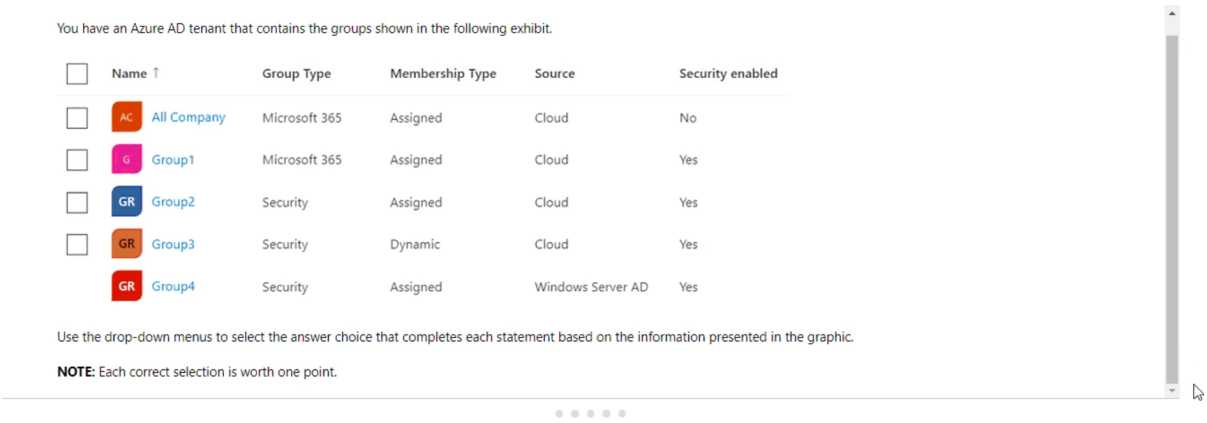
Number of days: 30

Role: User administrator

HOTSPOT

-

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



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

NOTE: Each correct selection is worth one point.

Answer Area

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

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

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

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

Correct Answer:

Answer Area

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

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

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

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

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

You plan to perform the following actions:

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

You need to create Group1.

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

NOTE: Each correct selection is worth one point.

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

B. Group type: Security -
Membership type: Assigned

C. Group type: Security -
Membership type: Dynamic User

D. Group type: Microsoft 365 -
Membership type: Dynamic User

E. Group type: Security -
Membership type: Dynamic Device

Correct Answer: *AB*

DRAG DROP
-

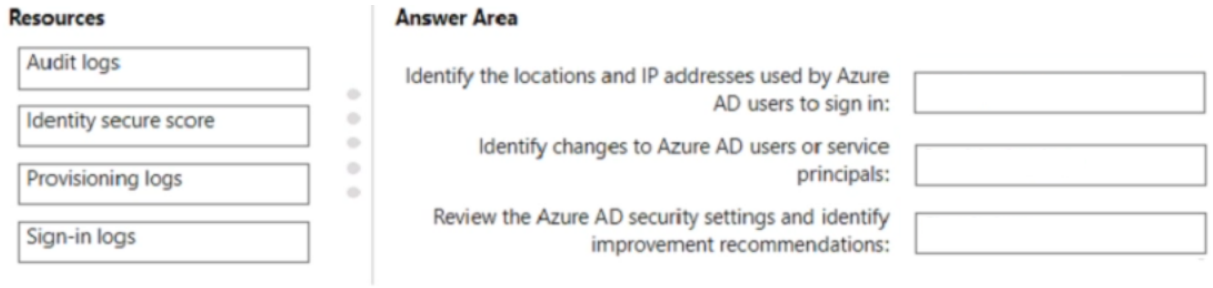
You have a Microsoft 365 E5 subscription.

You need to perform the following tasks:

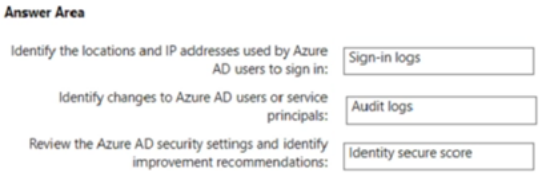
• Identify the locations and IP addresses used by Azure AD users to sign in.
• Review the Azure AD security settings and identify improvement recommendations.
• Identify changes to Azure AD users or service principals.

What should you use for each task? To answer, drag the appropriate resources to the correct requirements. Each resource may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



Correct Answer:



Question #1 *Topic 5*

Introductory Info

Case Study -

Overview -

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

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

Existing Environment. Existing Environment

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

Contoso_Resources. The Contoso_Resources OU contains all users and computers.

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

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

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

Existing Environment. Microsoft 365/Azure Environment

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

Microsoft Office 365 Enterprise E5

▪

Enterprise Mobility + Security E5

Windows 10 Enterprise E3

Project Plan 3

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

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

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

The users in the London office have the Microsoft 365 Phone System license unassigned.

The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

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

Existing Environment. Problem Statements

Contoso identifies the following issues:

Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.

The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.

The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.

Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.

When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes -

Contoso plans to implement the following changes:

Implement self-service password reset (SSPR).

Analyze Azure audit activity logs by using Azure Monitor.

Simplify license allocation for new users added to the tenant.

Collaborate with the users at Fabrikam on a joint marketing campaign.

Configure the User administrator role to require justification and approval to activate.

Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.
For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.
Contoso plans to acquire a company named ADatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.
Requirements. Technical Requirements
Contoso identifies the following technical requirements:
All users must be synced from AD DS to the contoso.com Azure AD tenant.
App1 must have a redirect URI pointed to https://contoso.com/auth-response.
License allocation for new users must be assigned automatically based on the location of the user.
Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.
Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.
The helpdesk administrators must be able to manage licenses for only the users in their respective office.
Users must be forced to change their password if there is a probability that the users' identity was compromised.

Question
You need to allocate licenses to the new users from ADatum. The solution must meet the technical requirements.
Which type of object should you create?

A. a Dynamic User security group

B. a distribution group

C. an OU

D. an administrative unit

Correct Answer: *D*
An administrative unit is an Azure AD resource that can be a container for other Azure AD resources. An administrative unit can contain only users, groups, or devices.
Administrative units restrict permissions in a role to any portion of your organization that you define.

Deployment scenario -
It can be useful to restrict administrative scope by using administrative units in organizations that are made up of independent divisions of any kind. Consider the example of a large university that's made up of many autonomous schools (School of Business, School of Engineering, and so on). Each school has a team of IT admins who control access, manage users, and set policies for their school.
Scenario: Contoso plans to acquire a company named ADatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named
Adatum. The users will be located in London and Seattle.
Contoso identifies the following technical requirements: License allocation for new users must be assigned automatically based on the location of the user.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/roles/administrative-units

Introductory Info

Case Study -

Overview -

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

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

Existing Environment. Existing Environment

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

Contoso_Resources. The Contoso_Resources OU contains all users and computers.

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

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

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

Existing Environment. Microsoft 365/Azure Environment

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

Microsoft Office 365 Enterprise E5

▪

Enterprise Mobility + Security E5

Windows 10 Enterprise E3

Project Plan 3

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

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

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

The users in the London office have the Microsoft 365 Phone System license unassigned.

The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

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

Existing Environment. Problem Statements

Contoso identifies the following issues:

Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.

The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.

The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.

Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.

When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes -

Contoso plans to implement the following changes:

Implement self-service password reset (SSPR).

Analyze Azure audit activity logs by using Azure Monitor.

Simplify license allocation for new users added to the tenant.

Collaborate with the users at Fabrikam on a joint marketing campaign.

Configure the User administrator role to require justification and approval to activate.

Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.

For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site,

group, and app.
Contoso plans to acquire a company named ADatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.
Requirements. Technical Requirements
Contoso identifies the following technical requirements:
All users must be synced from AD DS to the contoso.com Azure AD tenant.
App1 must have a redirect URI pointed to https://contoso.com/auth-response.
License allocation for new users must be assigned automatically based on the location of the user.
Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.
Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.
The helpdesk administrators must be able to manage licenses for only the users in their respective office.
Users must be forced to change their password if there is a probability that the users' identity was compromised.

Question
You need to sync the ADatum users. The solution must meet the technical requirements.
What should you do?

A. From the Microsoft Azure Active Directory Connect wizard, select Customize synchronization options.

B. From PowerShell, run Set-ADSyncScheduler.

C. From PowerShell, run Start-ADSyncSyncCycle.

D. From the Microsoft Azure Active Directory Connect wizard, select Change user sign-in.

Correct Answer: *A*
You need to select Customize synchronization options to configure Azure AD Connect to sync the Adatum organizational unit (OU).

Introductory Info

Case Study -

Overview -

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

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

Existing Environment. Existing Environment

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

Contoso_Resources. The Contoso_Resources OU contains all users and computers.

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

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

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

Existing Environment. Microsoft 365/Azure Environment

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

Microsoft Office 365 Enterprise E5

▪

Enterprise Mobility + Security E5

Windows 10 Enterprise E3

Project Plan 3

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

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

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

The users in the London office have the Microsoft 365 Phone System license unassigned.

The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

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

Existing Environment. Problem Statements

Contoso identifies the following issues:

Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.

The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.

The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.

Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.

When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes -

Contoso plans to implement the following changes:

Implement self-service password reset (SSPR).

Analyze Azure audit activity logs by using Azure Monitor.

Simplify license allocation for new users added to the tenant.

Collaborate with the users at Fabrikam on a joint marketing campaign.

Configure the User administrator role to require justification and approval to activate.

Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.

For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site,

group, and app.

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

Requirements. Technical Requirements

Contoso identifies the following technical requirements:

All users must be synced from AD DS to the contoso.com Azure AD tenant.

App1 must have a redirect URI pointed to https://contoso.com/auth-response.

License allocation for new users must be assigned automatically based on the location of the user.

Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.

Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.

The helpdesk administrators must be able to manage licenses for only the users in their respective office.

Users must be forced to change their password if there is a probability that the users' identity was compromised.

Question

HOTSPOT -

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Object to create for each branch office:

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

Tool to use:

- Azure Active Directory admin center
- Active Directory Administrative Center
- Active Directory module for Windows PowerShell
- Microsoft 365 admin center

Correct Answer:

Answer Area

Object to create for each branch office:

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

Tool to use:

- Azure Active Directory admin center
- Active Directory Administrative Center
- Active Directory module for Windows PowerShell
- Microsoft 365 admin center

Reference:

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

Introductory Info

Case Study -

Overview -

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

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

Existing Environment. Existing Environment

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

Contoso_Resources. The Contoso_Resources OU contains all users and computers.

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

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

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

Existing Environment. Microsoft 365/Azure Environment

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

Microsoft Office 365 Enterprise E5

▪

Enterprise Mobility + Security E5

Windows 10 Enterprise E3

Project Plan 3

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

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

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

The users in the London office have the Microsoft 365 Phone System license unassigned.

The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

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

Existing Environment. Problem Statements

Contoso identifies the following issues:

Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.

The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.

The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.

Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.

When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes -

Contoso plans to implement the following changes:

Implement self-service password reset (SSPR).

Analyze Azure audit activity logs by using Azure Monitor.

Simplify license allocation for new users added to the tenant.

Collaborate with the users at Fabrikam on a joint marketing campaign.

Configure the User administrator role to require justification and approval to activate.

Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.

For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site,

group, and app.
Contoso plans to acquire a company named ADatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.
Requirements. Technical Requirements
Contoso identifies the following technical requirements:
All users must be synced from AD DS to the contoso.com Azure AD tenant.
App1 must have a redirect URI pointed to https://contoso.com/auth-response.
License allocation for new users must be assigned automatically based on the location of the user.
Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.
Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.
The helpdesk administrators must be able to manage licenses for only the users in their respective office.
Users must be forced to change their password if there is a probability that the users' identity was compromised.

Question
You need to resolve the issue of the sales department users.
What should you configure for the Azure AD tenant?

A. the Device settings

B. the Access reviews settings

C. the User settings

D. Security defaults

Correct Answer: *C*
Scenario: There are Sales department users in London and in Seattle.
* The users in the London office have the Microsoft 365 Phone System license unassigned.
* The users in the Seattle office have the Yammer Enterprise license unassigned.
Use the Active users page to unassign licenses.
When you use the Active users page to unassign licenses, you unassign product licenses from users.
Unassign licenses from one user.
1. In the admin center, go to the Users > Active users page.
2. Select the row of the user that you want to unassign a license for.
3. In the right pane, select Licenses and Apps.
4. Expand the Licenses section, clear the boxes for the licenses that you want to unassign, then select Save changes.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/admin/manage/remove-licenses-from-users

Question #1 *Topic 6*

Introductory Info

Case Study -

Overview -

Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.

Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

Existing Environment. Identity Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD

Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

Existing Environment. Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active

Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller for litware.com
SERVER1	Windows Server 2019	Boston	Member server in litware.com that runs the Azure AD Application Proxy connector
SERVER2	Windows Server 2019	Boston	Member server that uses Azure AD Connect

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.

Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).

Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.

Use custom programs for Identity Governance.

Ensure that User1 can create enterprise applications in Azure AD.

Use the principle of least privilege.

Requirements. Licensing Requirements

Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest. Litware wants to manage the assignment of Azure

AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to a

Microsoft 365 group that has the appropriate licenses assigned.

Requirements. Management Requirements

Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.

Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

Implement multi-factor authentication (MFA) for all Litware users by using conditional access policies.

Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.

.

Implement a banned password list for the litware.com forest.

Enforce MFA when accessing on-premises applications.

Automatically detect and remediate externally leaked credentials.

Requirements. Access Requirements

Litware identifies the following access requirements:

Control all access to all Azure resources and Azure AD applications by using conditional access policies.

Implement a conditional access policy that has session controls for Microsoft SharePoint Online.

Control privileged access to applications by using access reviews in Azure AD.

Requirements. Monitoring Requirements

Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged attacks that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity.

Question

HOTSPOT -

You need to configure the assignment of Azure AD licenses to the Litware users. The solution must meet the licensing requirements.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Azure AD Connect settings to modify:

- Directory Extensions
- Domain Filtering
- Optional Features

Assign Azure AD licenses to:

- An Azure Active Directory group that has only nested groups
- An Azure Active Directory group that has the Assigned membership type
- An Azure Active Directory group that has the Dynamic User membership type

Correct Answer:

Answer Area

Azure AD Connect settings to modify:

- Directory Extensions
- Domain Filtering
- Optional Features

Assign Azure AD licenses to:

- An Azure Active Directory group that has only nested groups
- An Azure Active Directory group that has the Assigned membership type
- An Azure Active Directory group that has the Dynamic User membership type

Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest. Litware wants to manage the assignment of Azure

AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to a

Microsoft 365 group that has the appropriate licenses assigned.

Introductory Info

Case Study -

Overview -

Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.

Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

Existing Environment. Identity Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD

Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

Existing Environment. Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active

Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller for litware.com
SERVER1	Windows Server 2019	Boston	Member server in litware.com that runs the Azure AD Application Proxy connector
SERVER2	Windows Server 2019	Boston	Member server that uses Azure AD Connect

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.

Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).

Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.

Use custom programs for Identity Governance.

Ensure that User1 can create enterprise applications in Azure AD.

Use the principle of least privilege.

Requirements. Licensing Requirements

Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest. Litware wants to manage the assignment of Azure

AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to a

Microsoft 365 group that has the appropriate licenses assigned.

Requirements. Management Requirements

Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.

Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

Implement multi-factor authentication (MFA) for all Litware users by using conditional access policies.

Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.

▪

Implement a banned password list for the litware.com forest.

Enforce MFA when accessing on-premises applications.

Automatically detect and remediate externally leaked credentials.
Requirements. Access Requirements
Litware identifies the following access requirements:
Control all access to all Azure resources and Azure AD applications by using conditional access policies.
Implement a conditional access policy that has session controls for Microsoft SharePoint Online.
Control privileged access to applications by using access reviews in Azure AD.
Requirements. Monitoring Requirements
Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged attacks that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity.

Question
You need to meet the authentication requirements for leaked credentials.
What should you do?

A. Enable password hash synchronization in Azure AD Connect.

B. Configure Azure AD Password Protection.

C. Configure an authentication method policy in Azure AD.

D. Enable federation with PingFederate in Azure AD Connect.

Correct Answer: *A*
Reference:
https://docs.microsoft.com/en-us/azure/security/fundamentals/steps-secure-identity

Introductory Info

Case Study -

Overview -

Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.

Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

Existing Environment. Identity Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD

Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

Existing Environment. Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active

Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller for litware.com
SERVER1	Windows Server 2019	Boston	Member server in litware.com that runs the Azure AD Application Proxy connector
SERVER2	Windows Server 2019	Boston	Member server that uses Azure AD Connect

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.

Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).

Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.

Use custom programs for Identity Governance.

Ensure that User1 can create enterprise applications in Azure AD.

Use the principle of least privilege.

Requirements. Licensing Requirements

Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest. Litware wants to manage the assignment of Azure

AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to a

Microsoft 365 group that has the appropriate licenses assigned.

Requirements. Management Requirements

Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.

Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

Implement multi-factor authentication (MFA) for all Litware users by using conditional access policies.

Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.

▪

Implement a banned password list for the litware.com forest.

Enforce MFA when accessing on-premises applications.

Automatically detect and remediate externally leaked credentials.

Requirements. Access Requirements

Litware identifies the following access requirements:

Control all access to all Azure resources and Azure AD applications by using conditional access policies.

Implement a conditional access policy that has session controls for Microsoft SharePoint Online.

Control privileged access to applications by using access reviews in Azure AD.

Requirements. Monitoring Requirements

Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged attacks that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity.

Question

HOTSPOT -

You need to identify which roles to use for managing role assignments. The solution must meet the delegation requirements.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

To manage Azure AD built-in role assignments, use: [ ]
- Global administrator
- Privileged role administrator
- Security administrator
- User access administrator

To manage Azure built-in role assignments, use: [ ]
- Global administrator
- Privileged role administrator
- Security administrator
- User access administrator

Correct Answer:

Answer Area

To manage Azure AD built-in role assignments, use: [ ]
- Global administrator
- **Privileged role administrator**
- Security administrator
- User access administrator

To manage Azure built-in role assignments, use: [ ]
- Global administrator
- Privileged role administrator
- Security administrator
- **User access administrator**

Reference:

https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

Introductory Info

Case Study -

Overview -

Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.

Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

Existing Environment. Identity Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD

Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

Existing Environment. Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active

Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller for litware.com
SERVER1	Windows Server 2019	Boston	Member server in litware.com that runs the Azure AD Application Proxy connector
SERVER2	Windows Server 2019	Boston	Member server that uses Azure AD Connect

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.

Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).

Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.

Use custom programs for Identity Governance.

Ensure that User1 can create enterprise applications in Azure AD.

Use the principle of least privilege.

Requirements. Licensing Requirements

Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest. Litware wants to manage the assignment of Azure

AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to a

Microsoft 365 group that has the appropriate licenses assigned.

Requirements. Management Requirements

Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.

Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

Implement multi-factor authentication (MFA) for all Litware users by using conditional access policies.

Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.

▪

Implement a banned password list for the litware.com forest.

Enforce MFA when accessing on-premises applications.

Automatically detect and remediate externally leaked credentials.

Requirements. Access Requirements

Litware identifies the following access requirements:

Control all access to all Azure resources and Azure AD applications by using conditional access policies.

Implement a conditional access policy that has session controls for Microsoft SharePoint Online.

Control privileged access to applications by using access reviews in Azure AD.

Requirements. Monitoring Requirements

Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged attacks that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity.

Question

HOTSPOT -

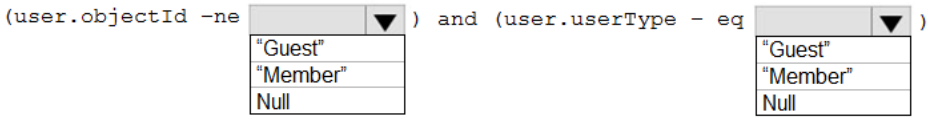
You need to create the LWGroup1 group to meet the management requirements.

How should you complete the dynamic membership rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

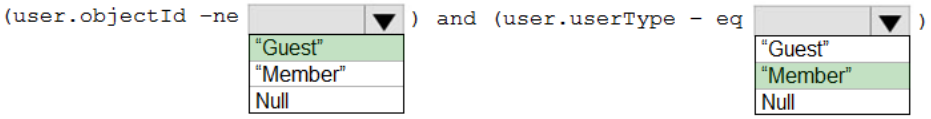
Hot Area:

Answer Area



Answer Area

Correct Answer:



Question #1 *Topic 7*

Introductory Info

Case Study -

Overview -

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

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

Existing Environment. Existing Environment

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

Contoso_Resources. The Contoso_Resources OU contains all users and computers.

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

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

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

Existing Environment. Microsoft 365/Azure Environment

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

Microsoft Office 365 Enterprise E5

▪

Enterprise Mobility + Security E5

Windows 10 Enterprise E3

Project Plan 3

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

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

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

The users in the London office have the Microsoft 365 Phone System license unassigned.

The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

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

Existing Environment. Problem Statements

Contoso identifies the following issues:

Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.

The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.

The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.

Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.

When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes -

Contoso plans to implement the following changes:

Implement self-service password reset (SSPR).

Analyze Azure audit activity logs by using Azure Monitor.

Simplify license allocation for new users added to the tenant.

Collaborate with the users at Fabrikam on a joint marketing campaign.

Configure the User administrator role to require justification and approval to activate.

Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.

For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

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

Requirements. Technical Requirements

Contoso identifies the following technical requirements:

All users must be synced from AD DS to the contoso.com Azure AD tenant.

App1 must have a redirect URI pointed to https://contoso.com/auth-response.

License allocation for new users must be assigned automatically based on the location of the user.

Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.

Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.

The helpdesk administrators must be able to manage licenses for only the users in their respective office.

Users must be forced to change their password if there is a probability that the users' identity was compromised.

Question

HOTSPOT -

You need to meet the technical requirements for the probability that user identities were compromised.

What should the users do first, and what should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

The users must first:

- Provide consent for any app to access the data of Contoso.
- Register for multi-factor authentication (MFA).
- Register for self-service password reset (SSPR).

You must configure:

- A sign-in risk policy
- A user risk policy
- An Azure AD Password Protection policy

Correct Answer:

Answer Area

The users must first:

- Provide consent for any app to access the data of Contoso.
- Register for multi-factor authentication (MFA).
- Register for self-service password reset (SSPR). ✓

You must configure:

- A sign-in risk policy
- A user risk policy ✓
- An Azure AD Password Protection policy

Reference:

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

Question #1 *Topic 8*

Introductory Info

Case Study -

Overview -

Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.

Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

Existing Environment. Identity Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD

Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

Existing Environment. Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active

Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller for litware.com
SERVER1	Windows Server 2019	Boston	Member server in litware.com that runs the Azure AD Application Proxy connector
SERVER2	Windows Server 2019	Boston	Member server that uses Azure AD Connect

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.

Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).

Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.

Use custom programs for Identity Governance.

Ensure that User1 can create enterprise applications in Azure AD.

Use the principle of least privilege.

Requirements. Licensing Requirements

Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest. Litware wants to manage the assignment of Azure

AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to a

Microsoft 365 group that has the appropriate licenses assigned.

Requirements. Management Requirements

Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.

Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

Implement multi-factor authentication (MFA) for all Litware users by using conditional access policies.

Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.

▪

Implement a banned password list for the litware.com forest.
Enforce MFA when accessing on-premises applications.
Automatically detect and remediate externally leaked credentials.
Requirements. Access Requirements
Litware identifies the following access requirements:
Control all access to all Azure resources and Azure AD applications by using conditional access policies.
Implement a conditional access policy that has session controls for Microsoft SharePoint Online.
Control privileged access to applications by using access reviews in Azure AD.
Requirements. Monitoring Requirements
Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged attacks that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity.

Question

You need to configure the MFA settings for users who connect from the Boston office. The solution must meet the authentication requirements and the access requirements.
What should you include in the configuration?

A. named locations that have a private IP address range

B. named locations that have a public IP address range

C. trusted IPs that have a public IP address range

D. trusted IPs that have a private IP address range

Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

Introductory Info

Case Study -

Overview -

Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.

Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

Existing Environment. Identity Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD

Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

Existing Environment. Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active

Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller for litware.com
SERVER1	Windows Server 2019	Boston	Member server in litware.com that runs the Azure AD Application Proxy connector
SERVER2	Windows Server 2019	Boston	Member server that uses Azure AD Connect

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.

Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).

Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.

Use custom programs for Identity Governance.

Ensure that User1 can create enterprise applications in Azure AD.

Use the principle of least privilege.

Requirements. Licensing Requirements

Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest. Litware wants to manage the assignment of Azure

AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to a

Microsoft 365 group that has the appropriate licenses assigned.

Requirements. Management Requirements

Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.

Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

Implement multi-factor authentication (MFA) for all Litware users by using conditional access policies.

Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.

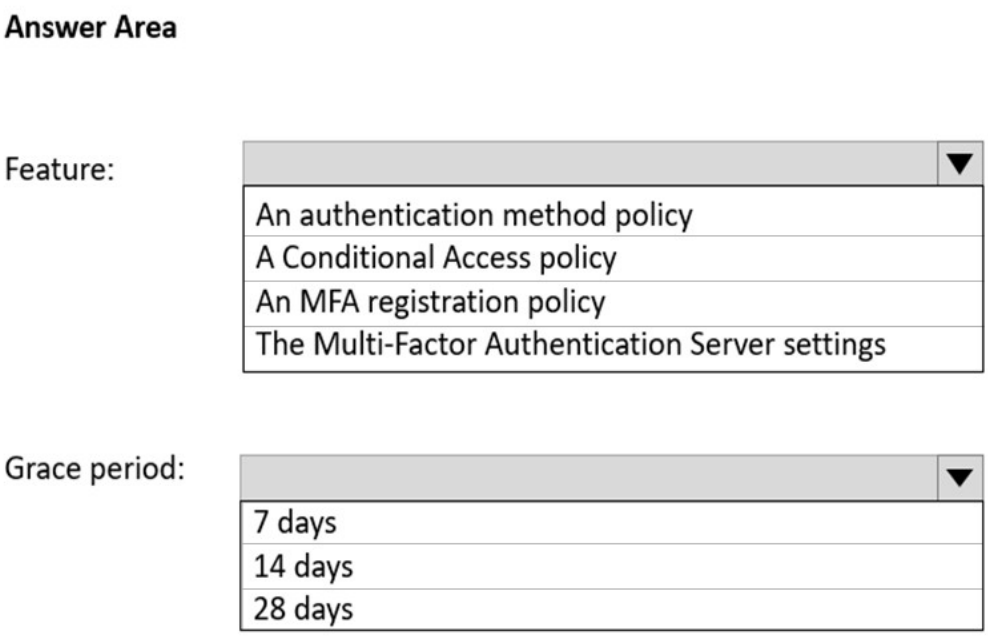
▪

Implement a banned password list for the litware.com forest.

Enforce MFA when accessing on-premises applications.

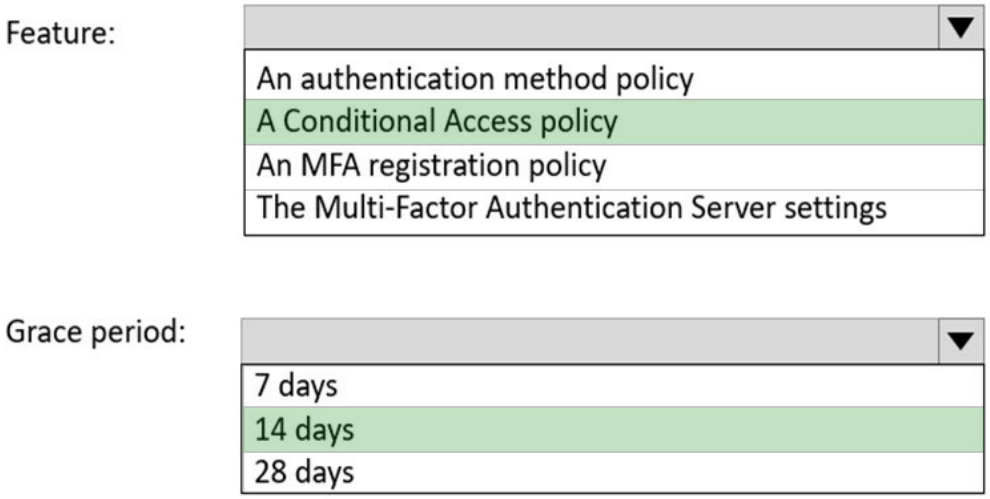
Automatically detect and remediate externally leaked credentials.
Requirements. Access Requirements
Litware identifies the following access requirements:
Control all access to all Azure resources and Azure AD applications by using conditional access policies.
Implement a conditional access policy that has session controls for Microsoft SharePoint Online.
Control privileged access to applications by using access reviews in Azure AD.
Requirements. Monitoring Requirements
Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged attacks that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity.

Question
HOTSPOT -
You need to support the planned changes and meet the technical requirements for MFA.
Which feature should you use, and how long before the users must complete the registration? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:



Correct Answer:

Answer Area



Box 1: A Conditional Access policy
Litware identifies the following authentication requirements:
Implement multi-factor authentication (MFA) for all Litware users by using conditional access policies.

Box 2: 14 days -
Multi-factor authentication (MFA): multi-factor authentication is a type of authentication that requires the use of two or more verification factors to gain access to a system. Azure MFA offers a 14 day grace period after being initiated.
Reference:
https://www.syskit.com/blog/using-azure-conditional-access-when-security-defaults-isnt-enough/

Question #1 *Topic 9*

Introductory Info

Case Study -

Overview -

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

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

Existing Environment. Existing Environment

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

Contoso_Resources. The Contoso_Resources OU contains all users and computers.

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

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

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

Existing Environment. Microsoft 365/Azure Environment

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

Microsoft Office 365 Enterprise E5

▪

Enterprise Mobility + Security E5

Windows 10 Enterprise E3

Project Plan 3

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

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

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

The users in the London office have the Microsoft 365 Phone System license unassigned.

The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

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

Existing Environment. Problem Statements

Contoso identifies the following issues:

Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.

The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.

The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.

Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.

When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes -

Contoso plans to implement the following changes:

Implement self-service password reset (SSPR).

Analyze Azure audit activity logs by using Azure Monitor.

Simplify license allocation for new users added to the tenant.

Collaborate with the users at Fabrikam on a joint marketing campaign.

Configure the User administrator role to require justification and approval to activate.

Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.
For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.
Contoso plans to acquire a company named ADatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.
Requirements. Technical Requirements
Contoso identifies the following technical requirements:
All users must be synced from AD DS to the contoso.com Azure AD tenant.
App1 must have a redirect URI pointed to https://contoso.com/auth-response.
License allocation for new users must be assigned automatically based on the location of the user.
Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.
Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.
The helpdesk administrators must be able to manage licenses for only the users in their respective office.
Users must be forced to change their password if there is a probability that the users' identity was compromised.

Question
You need to meet the planned changes and technical requirements for App1.
What should you implement?

A. a policy set in Microsoft Endpoint Manager

B. an app configuration policy in Microsoft Endpoint Manager

C. an app registration in Azure AD

D. Azure AD Application Proxy

Correct Answer: *C*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app

Question #1 *Topic 10*

Introductory Info

Case Study -

Overview -

Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.

Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

Existing Environment. Identity Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD

Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

Existing Environment. Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active

Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller for litware.com
SERVER1	Windows Server 2019	Boston	Member server in litware.com that runs the Azure AD Application Proxy connector
SERVER2	Windows Server 2019	Boston	Member server that uses Azure AD Connect

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.

Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).

Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.

Use custom programs for Identity Governance.

Ensure that User1 can create enterprise applications in Azure AD.

Use the principle of least privilege.

Requirements. Licensing Requirements

Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest. Litware wants to manage the assignment of Azure

AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to a

Microsoft 365 group that has the appropriate licenses assigned.

Requirements. Management Requirements

Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.

Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

Implement multi-factor authentication (MFA) for all Litware users by using conditional access policies.

Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.

.

Implement a banned password list for the litware.com forest.

Enforce MFA when accessing on-premises applications.

Automatically detect and remediate externally leaked credentials.

Requirements. Access Requirements

Litware identifies the following access requirements:

Control all access to all Azure resources and Azure AD applications by using conditional access policies.

Implement a conditional access policy that has session controls for Microsoft SharePoint Online.

Control privileged access to applications by using access reviews in Azure AD.

Requirements. Monitoring Requirements

Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged attacks that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity.

Question

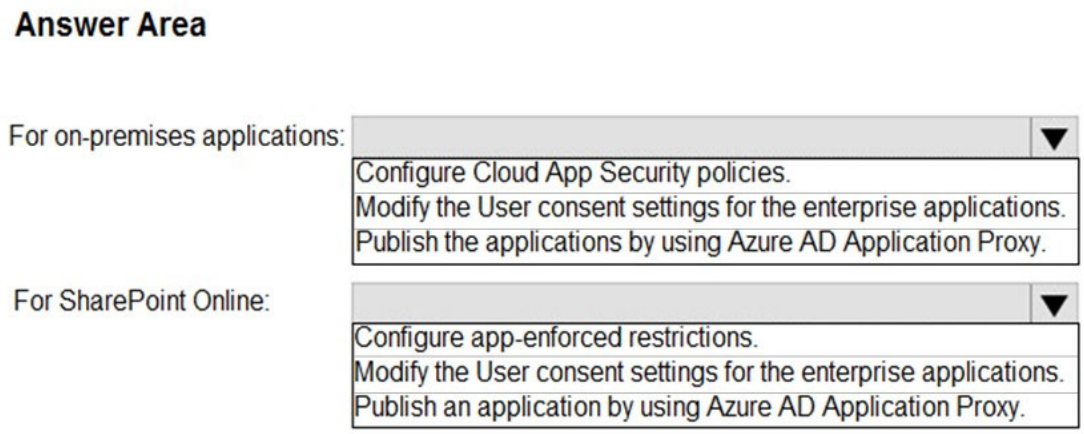
HOTSPOT -

You need to implement on-premises application and SharePoint Online restrictions to meet the authentication requirements and the access requirements.

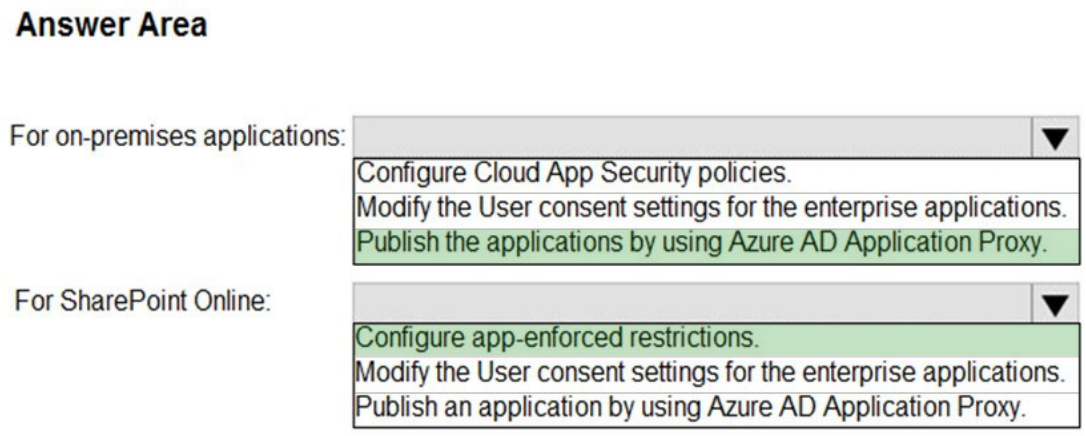
What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Reference:

https://docs.microsoft.com/en-us/sharepoint/app-enforced-restrictions https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session

Introductory Info

Case Study -

Overview -

Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.

Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

Existing Environment. Identity Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD

Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

Existing Environment. Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active

Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller for litware.com
SERVER1	Windows Server 2019	Boston	Member server in litware.com that runs the Azure AD Application Proxy connector
SERVER2	Windows Server 2019	Boston	Member server that uses Azure AD Connect

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.

Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).

Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.

Use custom programs for Identity Governance.

Ensure that User1 can create enterprise applications in Azure AD.

Use the principle of least privilege.

Requirements. Licensing Requirements

Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest. Litware wants to manage the assignment of Azure

AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to a

Microsoft 365 group that has the appropriate licenses assigned.

Requirements. Management Requirements

Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.

Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

Implement multi-factor authentication (MFA) for all Litware users by using conditional access policies.

Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.

▪

Implement a banned password list for the litware.com forest.

Enforce MFA when accessing on-premises applications.

Automatically detect and remediate externally leaked credentials.

Requirements. Access Requirements

Litware identifies the following access requirements:

Control all access to all Azure resources and Azure AD applications by using conditional access policies.

Implement a conditional access policy that has session controls for Microsoft SharePoint Online.

Control privileged access to applications by using access reviews in Azure AD.

Requirements. Monitoring Requirements

Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged attacks that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity.

Question

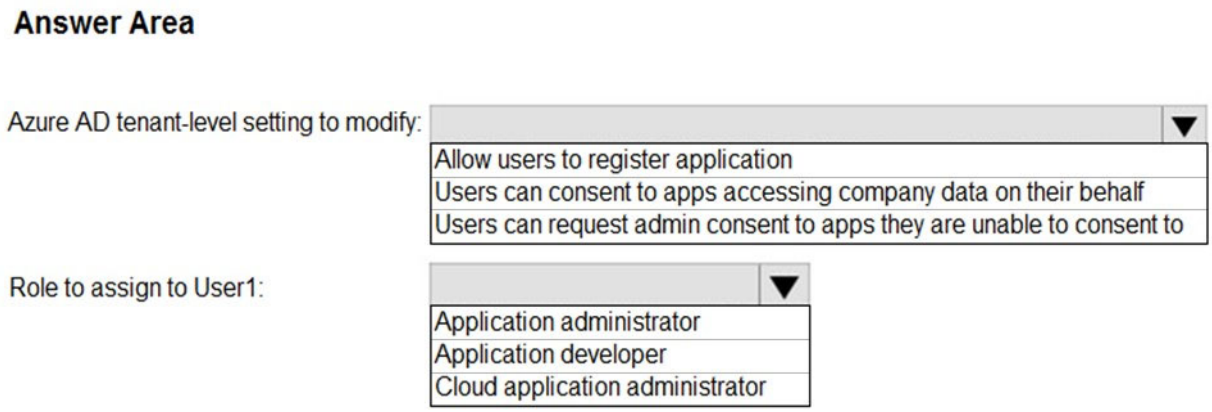
HOTSPOT -

You need to configure app registration in Azure AD to meet the delegation requirements.

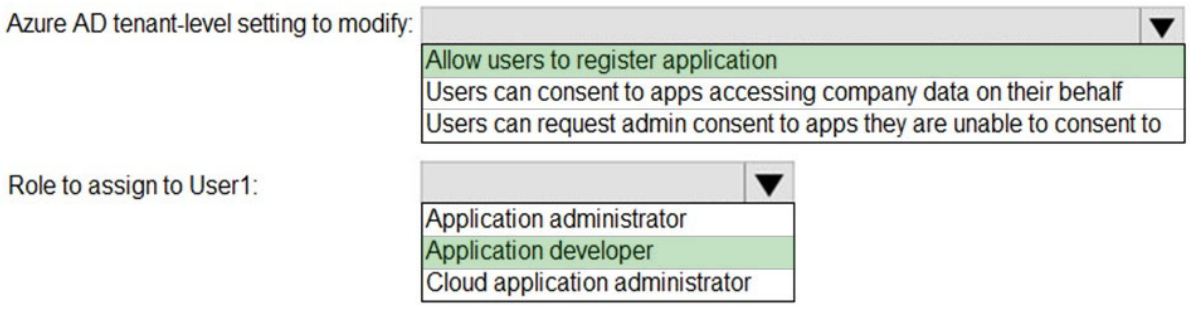
What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Reference:

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

Introductory Info

Case Study -

Overview -

Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.

Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

Existing Environment. Identity Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD

Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

Existing Environment. Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active

Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller for litware.com
SERVER1	Windows Server 2019	Boston	Member server in litware.com that runs the Azure AD Application Proxy connector
SERVER2	Windows Server 2019	Boston	Member server that uses Azure AD Connect

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.

Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).

Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.

Use custom programs for Identity Governance.

Ensure that User1 can create enterprise applications in Azure AD.

Use the principle of least privilege.

Requirements. Licensing Requirements

Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest. Litware wants to manage the assignment of Azure

AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to a

Microsoft 365 group that has the appropriate licenses assigned.

Requirements. Management Requirements

Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.

Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

Implement multi-factor authentication (MFA) for all Litware users by using conditional access policies.

Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.

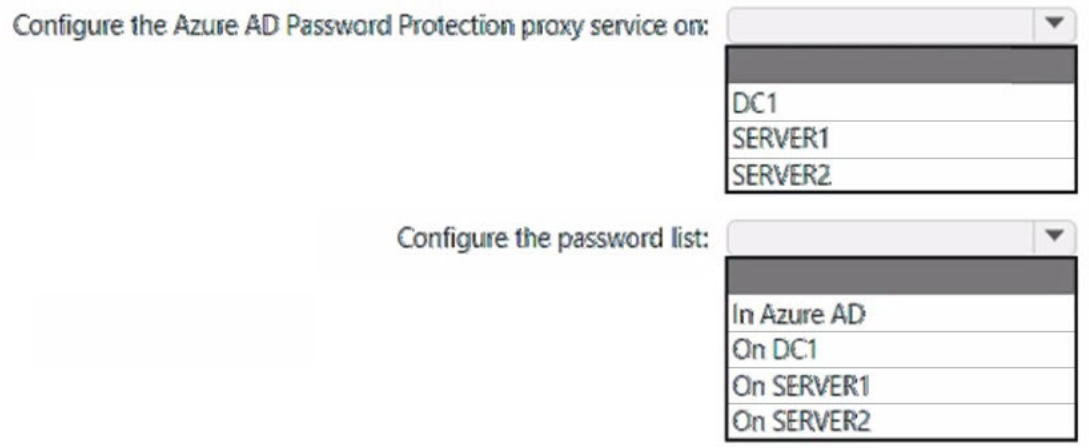
▪

Implement a banned password list for the litware.com forest.

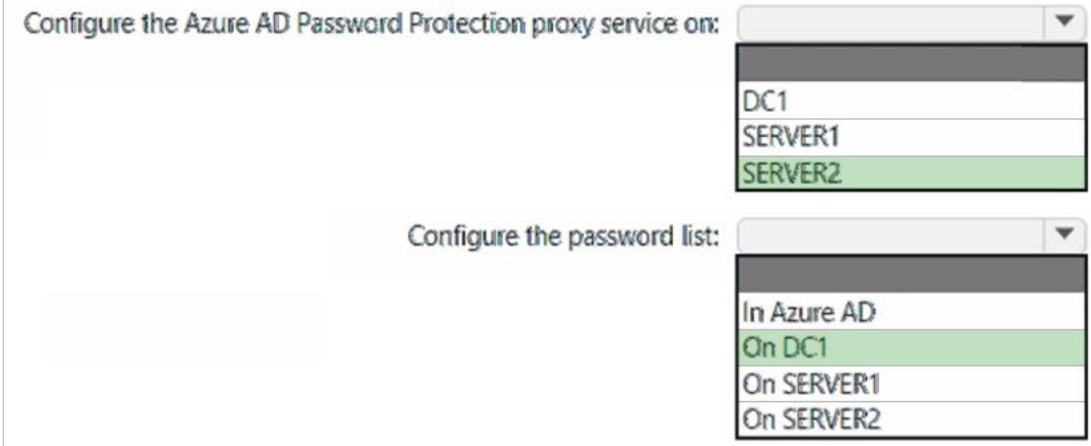
Enforce MFA when accessing on-premises applications.

Automatically detect and remediate externally leaked credentials.
Requirements. Access Requirements
Litware identifies the following access requirements:
Control all access to all Azure resources and Azure AD applications by using conditional access policies.
Implement a conditional access policy that has session controls for Microsoft SharePoint Online.
Control privileged access to applications by using access reviews in Azure AD.
Requirements. Monitoring Requirements
Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged attacks that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity.

Question
HOTSPOT -
How should the access be setup to the on-premises applications?
Hot Area:



Correct Answer:



Box 1: Server2 -
Incorrect:
Not Server 1: If you've deployed Azure AD Password Protection Proxy, do not install Azure AD Application Proxy and Azure AD Password Protection Proxy together on the same machine. Azure AD Application Proxy and Azure AD Password Protection Proxy install different versions of the Azure AD Connect Agent
Updater service. These different versions are incompatible when installed together on the same machine.
Server1 runs the Azure AD application Proxy connector.
To use Application Proxy, you need a Windows server running Windows Server 2012 R2 or later. You'll install the Application Proxy connector on the server. This connector server needs to connect to the Application Proxy services in Azure, and the on-premises applications that you plan to publish.
Scenario:
Requirements. Authentication Requirements include:
Enforce MFA when accessing on-premises applications.
Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller for litware.com
SERVER1	Windows Server 2019	Boston	Member server in litware.com that runs the Azure AD Application Proxy connector
SERVER2	Windows Server 2019	Boston	Member server that uses Azure AD Connect

Existing Environment. Identity Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD

Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Box 2: DC1 -

The Azure AD Password Protection proxy service is typically on a member server in your on-premises AD DS environment. Once installed, the Azure AD

Password Protection proxy service communicates with Azure AD to maintain a copy of the global and customer banned password lists for your Azure AD tenant.

Reference:

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

https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-add-on-premises-application

Question #1 *Topic 11*

Introductory Info

Case Study -

Overview -

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

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

Existing Environment. Existing Environment

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

Contoso_Resources. The Contoso_Resources OU contains all users and computers.

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

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

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

Existing Environment. Microsoft 365/Azure Environment

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

Microsoft Office 365 Enterprise E5

▪

Enterprise Mobility + Security E5

Windows 10 Enterprise E3

Project Plan 3

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

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

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

The users in the London office have the Microsoft 365 Phone System license unassigned.

The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

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

Existing Environment. Problem Statements

Contoso identifies the following issues:

Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.

The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.

The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.

Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.

When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes -

Contoso plans to implement the following changes:

Implement self-service password reset (SSPR).

Analyze Azure audit activity logs by using Azure Monitor.

Simplify license allocation for new users added to the tenant.

Collaborate with the users at Fabrikam on a joint marketing campaign.

Configure the User administrator role to require justification and approval to activate.

Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.
For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.
Contoso plans to acquire a company named ADatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.
Requirements. Technical Requirements
Contoso identifies the following technical requirements:
All users must be synced from AD DS to the contoso.com Azure AD tenant.
App1 must have a redirect URI pointed to https://contoso.com/auth-response.
License allocation for new users must be assigned automatically based on the location of the user.
Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.
Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.
The helpdesk administrators must be able to manage licenses for only the users in their respective office.
Users must be forced to change their password if there is a probability that the users' identity was compromised.

Question
You create a Log Analytics workspace.
You need to implement the technical requirements for auditing.
What should you configure in Azure AD?

A. Company branding

B. Diagnostics settings

C. External Identities

D. App registrations

Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/overview-monitoring

Introductory Info

Case Study -

Overview -

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

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

Existing Environment. Existing Environment

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

Contoso_Resources. The Contoso_Resources OU contains all users and computers.

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

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

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

Existing Environment. Microsoft 365/Azure Environment

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

Microsoft Office 365 Enterprise E5

▪

Enterprise Mobility + Security E5

Windows 10 Enterprise E3

Project Plan 3

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

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

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

The users in the London office have the Microsoft 365 Phone System license unassigned.

The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

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

Existing Environment. Problem Statements

Contoso identifies the following issues:

Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.

The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.

The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.

Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.

When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes -

Contoso plans to implement the following changes:

Implement self-service password reset (SSPR).

Analyze Azure audit activity logs by using Azure Monitor.

Simplify license allocation for new users added to the tenant.

Collaborate with the users at Fabrikam on a joint marketing campaign.

Configure the User administrator role to require justification and approval to activate.

Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.

For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site,

group, and app.

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

Requirements. Technical Requirements

Contoso identifies the following technical requirements:

All users must be synced from AD DS to the contoso.com Azure AD tenant.

App1 must have a redirect URI pointed to https://contoso.com/auth-response.

License allocation for new users must be assigned automatically based on the location of the user.

Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.

Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.

The helpdesk administrators must be able to manage licenses for only the users in their respective office.

Users must be forced to change their password if there is a probability that the users' identity was compromised.

Question

HOTSPOT -

You need to implement the planned changes and technical requirements for the marketing department.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

To configure user access: [ ]
- An access package
- An access review
- A conditional access policy

To enable collaboration with fabrikam.com: [ ]
- An accepted domain
- A connected organization
- A custom domain name

Answer Area

Correct Answer:

To configure user access: [An access package]
- An access package
- An access review
- A conditional access policy

To enable collaboration with fabrikam.com: [A connected organization]
- An accepted domain
- A connected organization
- A custom domain name

Reference:

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

Introductory Info

Case Study -

Overview -

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

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

Existing Environment. Existing Environment

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

Contoso_Resources. The Contoso_Resources OU contains all users and computers.

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

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

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

Existing Environment. Microsoft 365/Azure Environment

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

Microsoft Office 365 Enterprise E5

▪

Enterprise Mobility + Security E5

Windows 10 Enterprise E3

Project Plan 3

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

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

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

The users in the London office have the Microsoft 365 Phone System license unassigned.

The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

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

Existing Environment. Problem Statements

Contoso identifies the following issues:

Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.

The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.

The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.

Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.

When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes -

Contoso plans to implement the following changes:

Implement self-service password reset (SSPR).

Analyze Azure audit activity logs by using Azure Monitor.

Simplify license allocation for new users added to the tenant.

Collaborate with the users at Fabrikam on a joint marketing campaign.

Configure the User administrator role to require justification and approval to activate.

Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.

For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site,

group, and app.
Contoso plans to acquire a company named ADatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.
Requirements. Technical Requirements
Contoso identifies the following technical requirements:
All users must be synced from AD DS to the contoso.com Azure AD tenant.
App1 must have a redirect URI pointed to https://contoso.com/auth-response.
License allocation for new users must be assigned automatically based on the location of the user.
Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.
Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.
The helpdesk administrators must be able to manage licenses for only the users in their respective office.
Users must be forced to change their password if there is a probability that the users' identity was compromised.

Question
You need to meet the planned changes for the User administrator role.
What should you do?

A. Create an access review.

B. Create an administrative unit.

C. Modify Active assignments.

D. Modify Role settings.

Correct Answer: *C*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-add-role-to-user?tabs=new

Introductory Info

Case Study -

Overview -

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

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

Existing Environment. Existing Environment

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

Contoso_Resources. The Contoso_Resources OU contains all users and computers.

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

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

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

Existing Environment. Microsoft 365/Azure Environment

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

Microsoft Office 365 Enterprise E5

▪

Enterprise Mobility + Security E5

Windows 10 Enterprise E3

Project Plan 3

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

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

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

The users in the London office have the Microsoft 365 Phone System license unassigned.

The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

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

Existing Environment. Problem Statements

Contoso identifies the following issues:

Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.

The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.

The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.

Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.

When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes -

Contoso plans to implement the following changes:

Implement self-service password reset (SSPR).

Analyze Azure audit activity logs by using Azure Monitor.

Simplify license allocation for new users added to the tenant.

Collaborate with the users at Fabrikam on a joint marketing campaign.

Configure the User administrator role to require justification and approval to activate.

Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.

For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site,

group, and app.
Contoso plans to acquire a company named ADatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.
Requirements. Technical Requirements
Contoso identifies the following technical requirements:
All users must be synced from AD DS to the contoso.com Azure AD tenant.
App1 must have a redirect URI pointed to https://contoso.com/auth-response.
License allocation for new users must be assigned automatically based on the location of the user.
Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.
Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.
The helpdesk administrators must be able to manage licenses for only the users in their respective office.
Users must be forced to change their password if there is a probability that the users' identity was compromised.

Question
You need to modify the settings of the User administrator role to meet the technical requirements.
Which two actions should you perform for the role? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Select Require justification on activation.

B. Select Require ticket information on activation.

C. Modify the Expire eligible assignments after setting.

D. Set all assignments to Eligible.

E. Set all assignments to Active.

Correct Answer: *AE*
Scenario: Configure the User administrator role to require justification and approval to activate.
A: Require justification.
You can require that users enter a business justification when they activate. To require justification, check the Require justification on active assignment box or the
Require justification on activation box.
E: You can choose from two assignment duration options for each assignment type (eligible and active) when you configure settings for a role.
You can choose one of these active assignment duration options:
Allow permanent active assignment: Global admins and Privileged role admins can assign permanent active assignment.
Expire active assignment after: Global admins and Privileged role admins can require that all active assignments have a specified start and end date.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settings

Introductory Info

Case Study -

Overview -

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

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

Existing Environment. Existing Environment

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

Contoso_Resources. The Contoso_Resources OU contains all users and computers.

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

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

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

Existing Environment. Microsoft 365/Azure Environment

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

Microsoft Office 365 Enterprise E5

▪

Enterprise Mobility + Security E5

Windows 10 Enterprise E3

Project Plan 3

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

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

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

The users in the London office have the Microsoft 365 Phone System license unassigned.

The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

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

Existing Environment. Problem Statements

Contoso identifies the following issues:

Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.

The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.

The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.

Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.

When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes -

Contoso plans to implement the following changes:

Implement self-service password reset (SSPR).

Analyze Azure audit activity logs by using Azure Monitor.

Simplify license allocation for new users added to the tenant.

Collaborate with the users at Fabrikam on a joint marketing campaign.

Configure the User administrator role to require justification and approval to activate.

Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.

For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site,

group, and app.
Contoso plans to acquire a company named ADatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.
Requirements. Technical Requirements
Contoso identifies the following technical requirements:
All users must be synced from AD DS to the contoso.com Azure AD tenant.
App1 must have a redirect URI pointed to https://contoso.com/auth-response.
License allocation for new users must be assigned automatically based on the location of the user.
Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.
Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.
The helpdesk administrators must be able to manage licenses for only the users in their respective office.
Users must be forced to change their password if there is a probability that the users' identity was compromised.

Question
You need to resolve the issue of the guest user invitations.
What should you do for the Azure AD tenant?

A. Configure the Continuous access evaluation settings.

B. Configure a Conditional Access policy.

C. Configure the Access reviews settings.

D. Modify the External collaboration settings.

Correct Answer: *C*
Scenario: The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.
Manage guest access with Azure AD access reviews.
With Azure Active Directory (Azure AD), you can easily enable collaboration across organizational boundaries by using the Azure AD B2B feature. Guest users from other tenants can be invited by administrators or by other users. This capability also applies to social identities such as Microsoft accounts.
You also can easily ensure that guest users have appropriate access. You can ask the guests themselves or a decision maker to participate in an access review and recertify (or attest) to the guests' access. The reviewers can give their input on each user's need for continued access, based on suggestions from Azure AD.
When an access review is finished, you can then make changes and remove access for guests who no longer need it.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/governance/manage-guest-access-with-access-reviews

Introductory Info

Case Study -

Overview -

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

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

Existing Environment. Existing Environment

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

Contoso_Resources. The Contoso_Resources OU contains all users and computers.

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

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

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

Existing Environment. Microsoft 365/Azure Environment

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

Microsoft Office 365 Enterprise E5

▪

Enterprise Mobility + Security E5

Windows 10 Enterprise E3

Project Plan 3

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

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

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

The users in the London office have the Microsoft 365 Phone System license unassigned.

The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

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

Existing Environment. Problem Statements

Contoso identifies the following issues:

Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.

The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.

The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.

Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.

When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes -

Contoso plans to implement the following changes:

Implement self-service password reset (SSPR).

Analyze Azure audit activity logs by using Azure Monitor.

Simplify license allocation for new users added to the tenant.

Collaborate with the users at Fabrikam on a joint marketing campaign.

Configure the User administrator role to require justification and approval to activate.

Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.

For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site,

group, and app.
Contoso plans to acquire a company named ADatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.
Requirements. Technical Requirements
Contoso identifies the following technical requirements:
All users must be synced from AD DS to the contoso.com Azure AD tenant.
App1 must have a redirect URI pointed to https://contoso.com/auth-response.
License allocation for new users must be assigned automatically based on the location of the user.
Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.
Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.
The helpdesk administrators must be able to manage licenses for only the users in their respective office.
Users must be forced to change their password if there is a probability that the users' identity was compromised.

Question
You need to sync the ADatum users. The solution must meet the technical requirements.
What should you do?

A. From the Microsoft Azure Active Directory Connect wizard, select Customize synchronization options.

B. From PowerShell, run Set-ADSyncScheduler.

C. From PowerShell, run Start-ADSyncSyncCycle.

D. From the Microsoft Azure Active Directory Connect wizard, select Change user sign-in.

Correct Answer: *A*
You need to select Customize synchronization options to configure Azure AD Connect to sync the Adatum organizational unit (OU).

Question #1 *Topic 12*

Introductory Info

Case Study -

Overview -

Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.

Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

Existing Environment. Identity Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD

Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

Existing Environment. Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active

Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller for litware.com
SERVER1	Windows Server 2019	Boston	Member server in litware.com that runs the Azure AD Application Proxy connector
SERVER2	Windows Server 2019	Boston	Member server that uses Azure AD Connect

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.

Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).

Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.

Use custom programs for Identity Governance.

Ensure that User1 can create enterprise applications in Azure AD.

Use the principle of least privilege.

Requirements. Licensing Requirements

Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest. Litware wants to manage the assignment of Azure

AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to a

Microsoft 365 group that has the appropriate licenses assigned.

Requirements. Management Requirements

Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.

Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

Implement multi-factor authentication (MFA) for all Litware users by using conditional access policies.

Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.

.

Implement a banned password list for the litware.com forest.
Enforce MFA when accessing on-premises applications.
Automatically detect and remediate externally leaked credentials.
Requirements. Access Requirements
Litware identifies the following access requirements:
Control all access to all Azure resources and Azure AD applications by using conditional access policies.
Implement a conditional access policy that has session controls for Microsoft SharePoint Online.
Control privileged access to applications by using access reviews in Azure AD.
Requirements. Monitoring Requirements
Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged attacks that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity.

Question

You need to configure the detection of multi-staged attacks to meet the monitoring requirements.
What should you do?

A. Customize the Microsoft Sentinel rule logic.

B. Create a workbook.

C. Add Microsoft Sentinel data connectors.

D. Add an Microsoft Sentinel playbook.

Correct Answer: *A*

Introductory Info

Case Study -

Overview -

Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.

Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

Existing Environment. Identity Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD

Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

Existing Environment. Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active

Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller for litware.com
SERVER1	Windows Server 2019	Boston	Member server in litware.com that runs the Azure AD Application Proxy connector
SERVER2	Windows Server 2019	Boston	Member server that uses Azure AD Connect

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.

Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).

Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.

Use custom programs for Identity Governance.

Ensure that User1 can create enterprise applications in Azure AD.

Use the principle of least privilege.

Requirements. Licensing Requirements

Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest. Litware wants to manage the assignment of Azure

AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to a

Microsoft 365 group that has the appropriate licenses assigned.

Requirements. Management Requirements

Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.

Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

Implement multi-factor authentication (MFA) for all Litware users by using conditional access policies.

Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.

▪

Implement a banned password list for the litware.com forest.

Enforce MFA when accessing on-premises applications.

Automatically detect and remediate externally leaked credentials.
Requirements. Access Requirements
Litware identifies the following access requirements:
Control all access to all Azure resources and Azure AD applications by using conditional access policies.
Implement a conditional access policy that has session controls for Microsoft SharePoint Online.
Control privileged access to applications by using access reviews in Azure AD.
Requirements. Monitoring Requirements
Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged attacks that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity.

Question
You need to track application access assignments by using Identity Governance. The solution must meet the delegation requirements.
What should you do first?

A. Modify the User consent settings for the enterprise applications.

B. Create a catalog.

C. Create a program.

D. Modify the Admin consent requests settings for the enterprise applications.

Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-overview