Microsoft Identity and Access Administrator

Exam Code: SC-300

Version: 2022

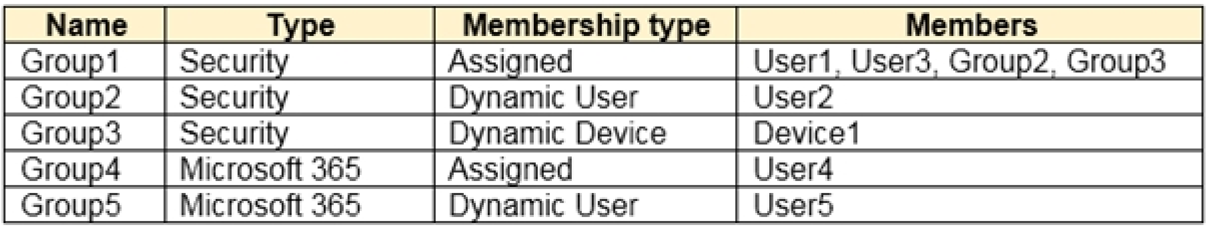
Prepared by MA

Question #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 computers for Azure AD Seamless SSO.
What should you do?

- A. Configure Sign-in options.
- B. Enable Enterprise State Roaming.
- **C**. Modify the Intranet Zone settings.
- D. Install the Azure AD Connect Authentication Agent.

Question #2*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

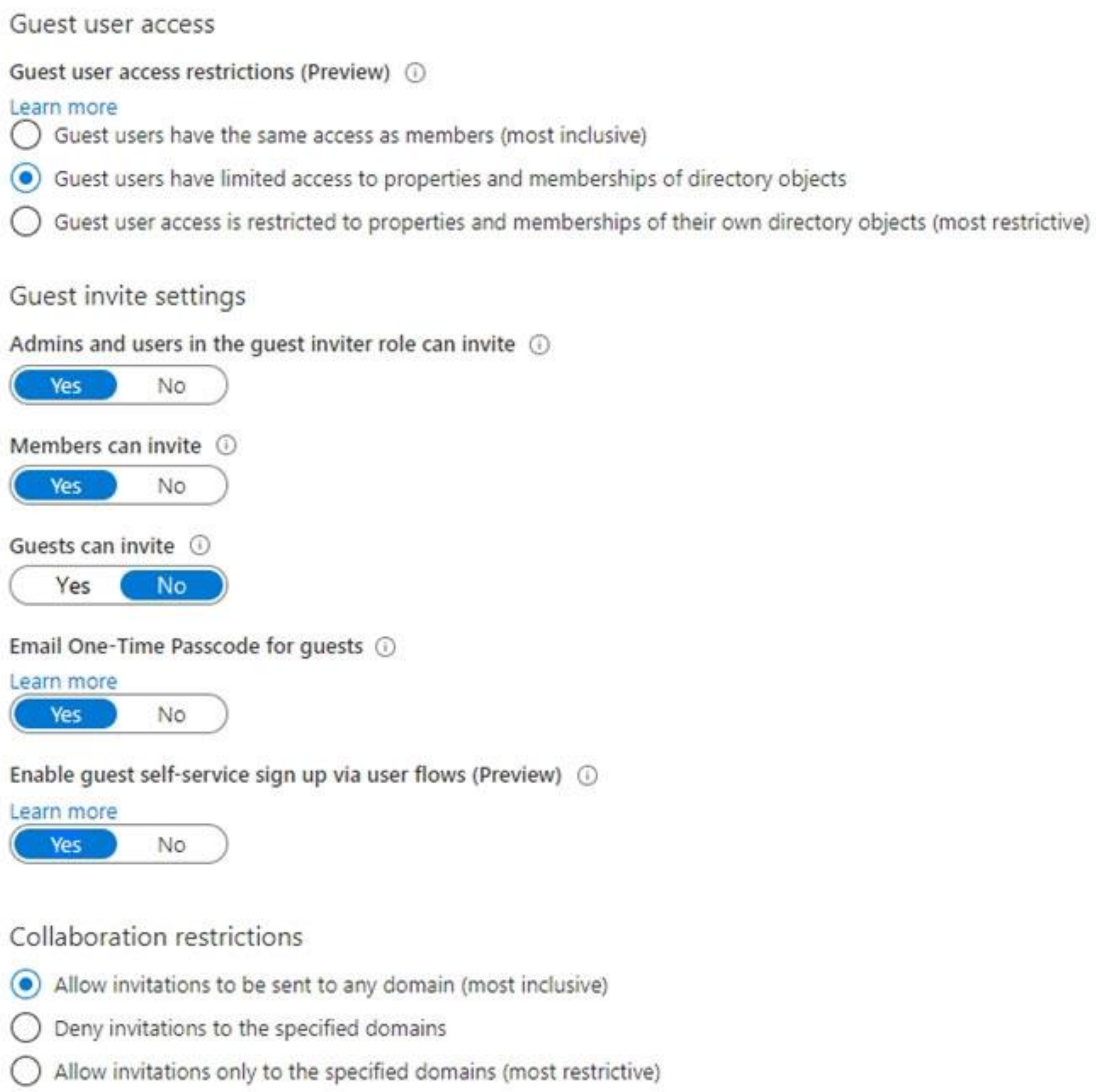
Question #3

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

Question #4*Topic 1*

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



Guest user access

Guest user access restrictions (Preview) ⓘ

Learn more

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

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

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

Guest invite settings

Admins and users in the guest inviter role can invite ⓘ

[✓ Yes] No

Members can invite ⓘ

[✓ Yes] No

Guests can invite ⓘ

Yes [✓ No]

Email One-Time Passcode for guests ⓘ

Learn more

[✓ Yes] No

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

Learn more

[✓ Yes] No

Collaboration restrictions

● Allow invitations to be sent to any domain (most inclusive)

○ Deny invitations to the specified domains

○ Allow invitations only to the specified domains (most restrictive)

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

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

Which users will be emailed a passcode?

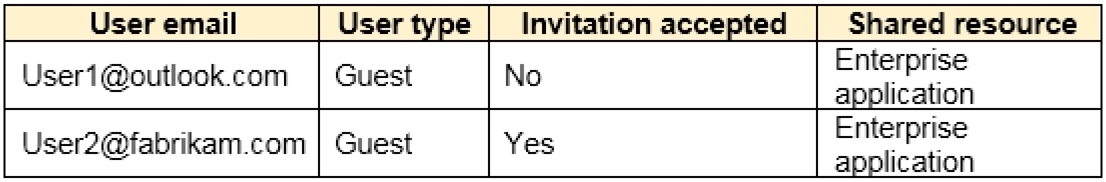
- **A**. User2 only
- B. User1 only
- C. User1 and User2 only
- D. User1, User2, and User3

Question #5

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?

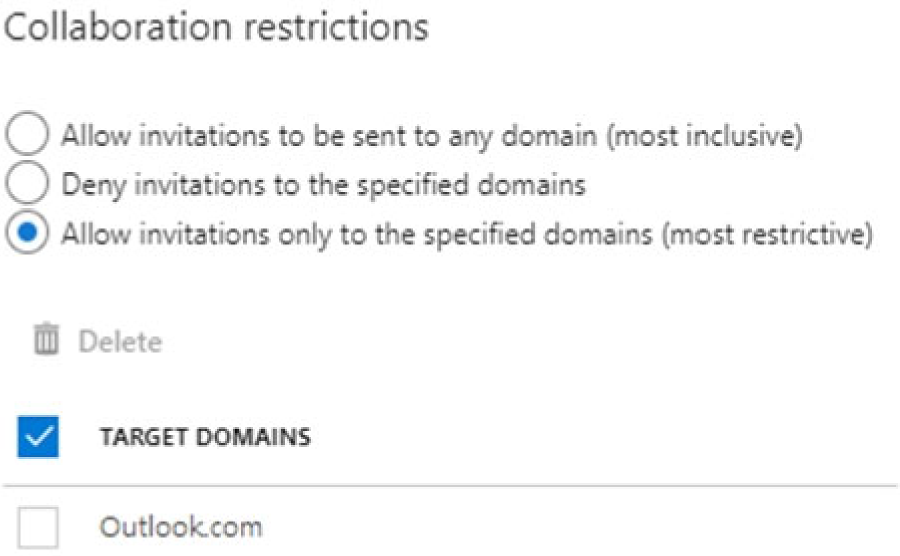
- A. the Identity Governance blade in the Azure Active Directory admin center
- B. the Set-AzureAdUser cmdlet
- **C.** the Licenses blade in the Azure Active Directory admin center
- D. the Set-WindowsProductKey cmdlet

Question #6*Topic 1*
HOTSPOT -
You have a Microsoft 365 tenant named contoso.com.
Guest user access is enabled.
Users are invited to collaborate with contoso.com as shown in the following table.



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

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



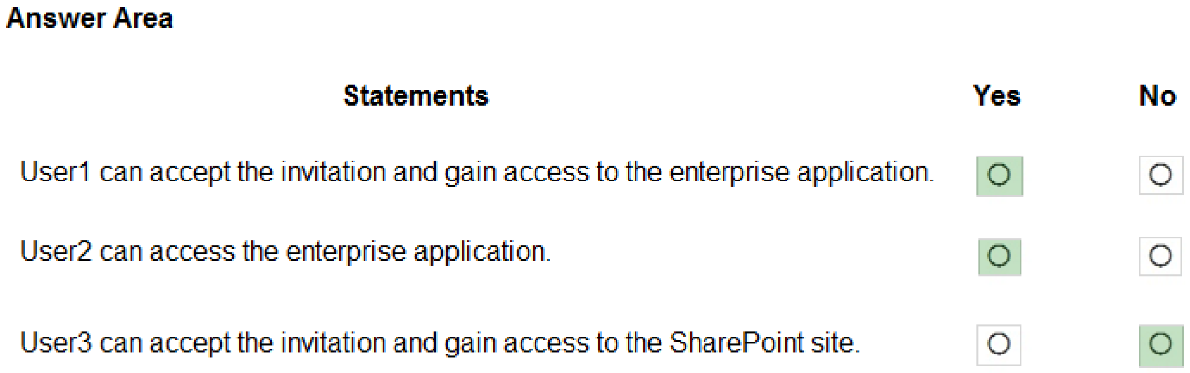
Collaboration restrictions

○ Allow invitations to be sent to any domain (most inclusive)
○ Deny invitations to the specified domains
● Allow invitations only to the specified domains (most restrictive)

☑ TARGET DOMAINS

□ Outlook.com

From a Microsoft SharePoint Online site, a user invites user3@adatum.com to the site.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:



Answer Area

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

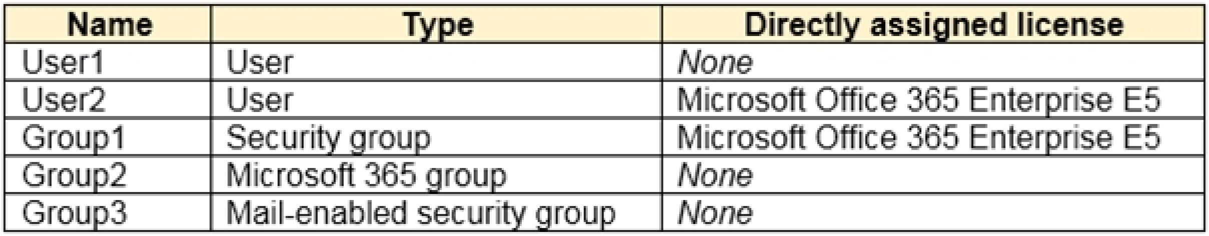
Question #7

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

Question #8

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

Question #9

DRAG DROP -

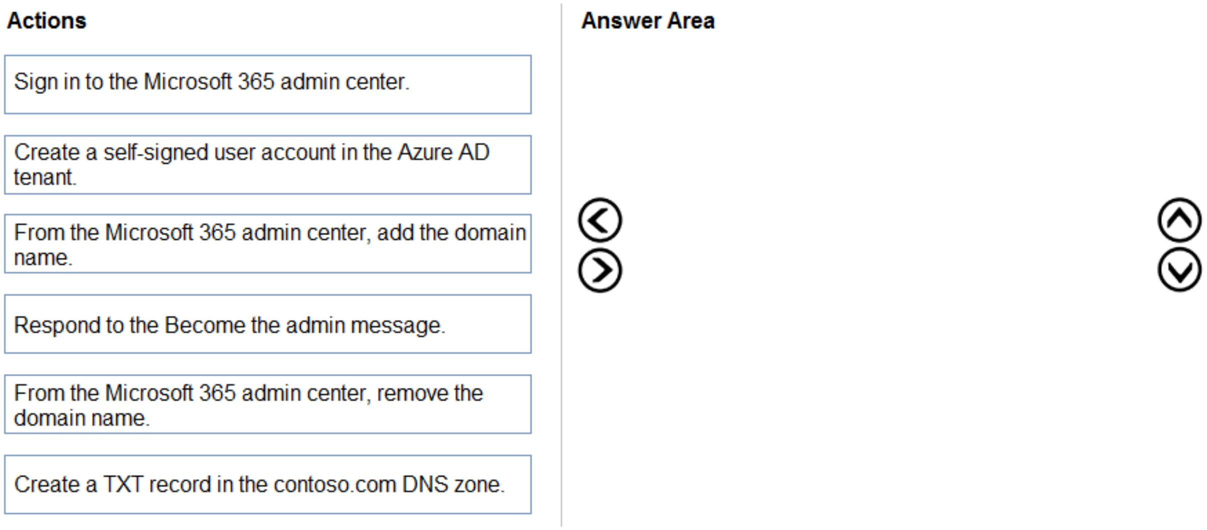
You have an on-premises Microsoft Exchange organization that uses an SMTP address space of contoso.com.

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

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

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

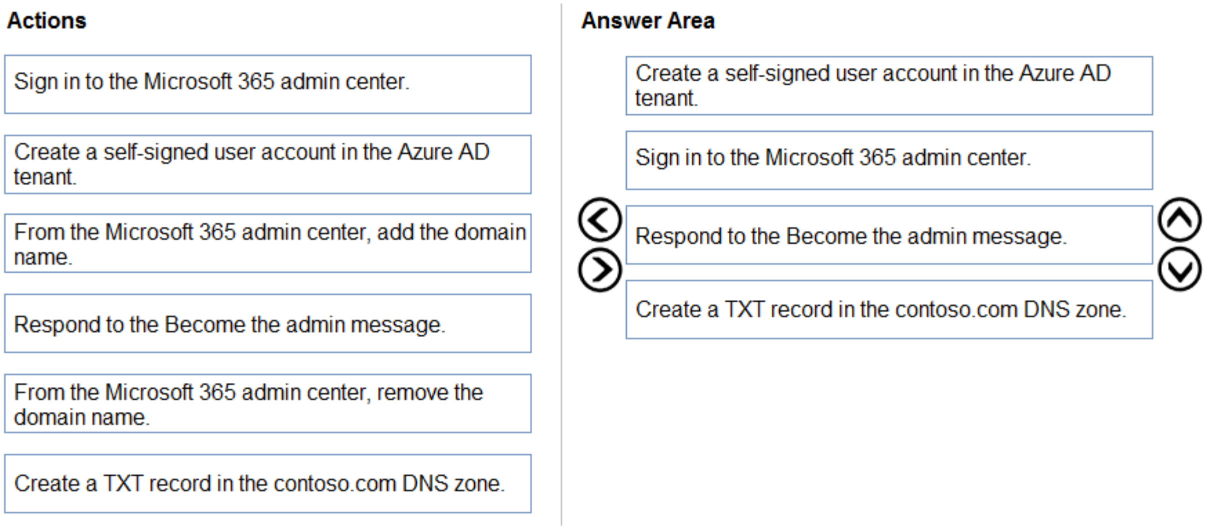
Select and Place:



Actions

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

Answer Area



Actions

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

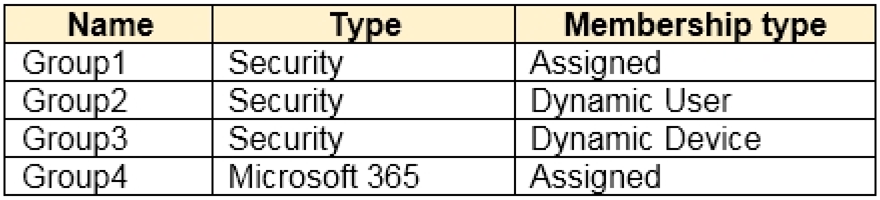
Answer Area

- Create a self-signed user account in the Azure AD tenant.
- Sign in to the Microsoft 365 admin center.
- Respond to the Become the admin message.
- Create a TXT record in the contoso.com DNS zone.

Question #10

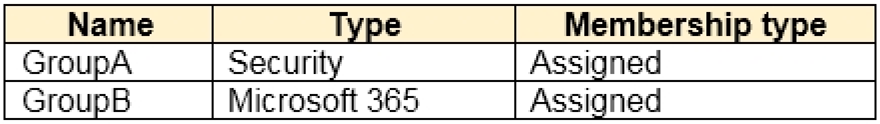
HOTSPOT -

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.

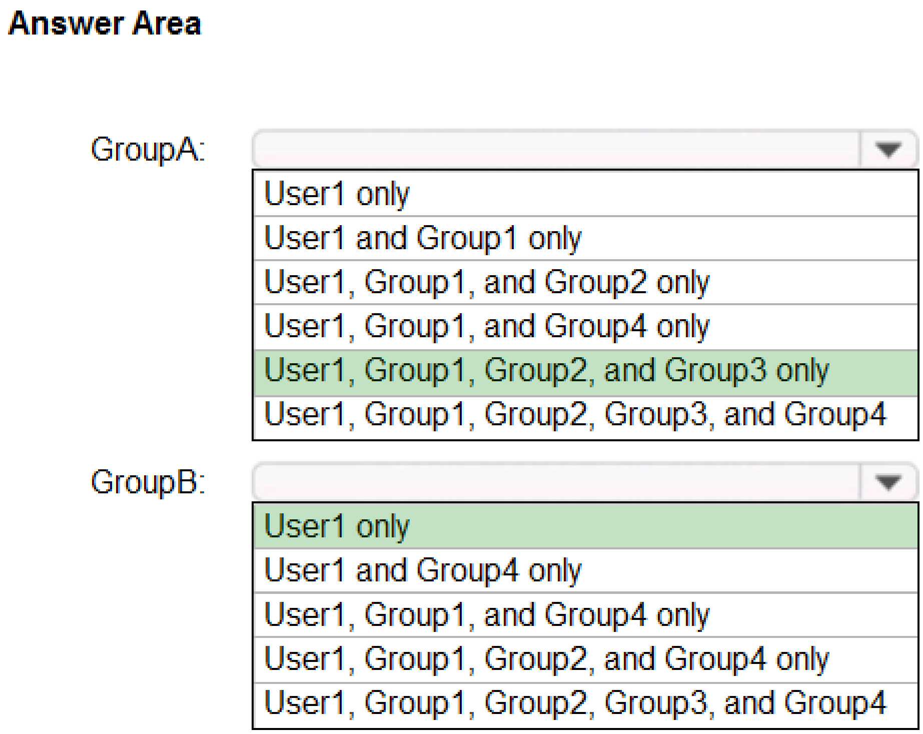


Name	Type	Membership type
GroupA	Security	Assigned
GroupB	Microsoft 365	Assigned

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

Question #11

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

- A. Yes
- **B**. No

Question #12
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an 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

Question #13

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?

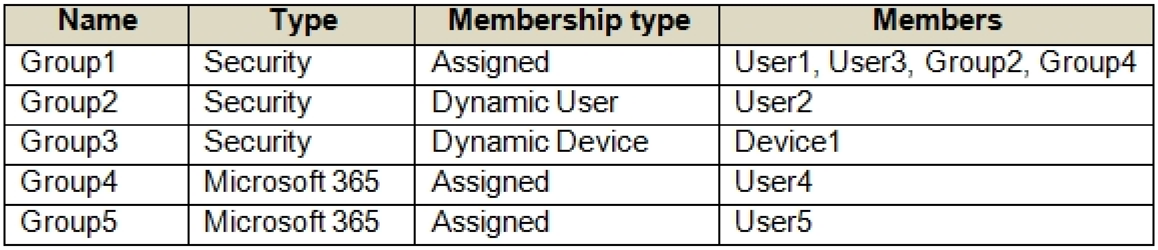
- A. Yes
- **B.** No

Question #14
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

Question #15

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

Question #16
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.

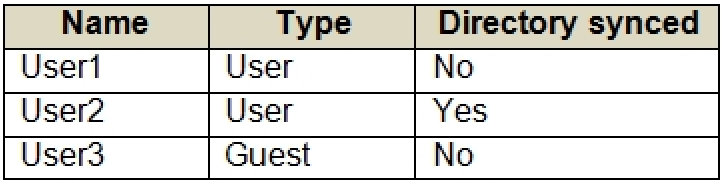
Question #17

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.

Question #18

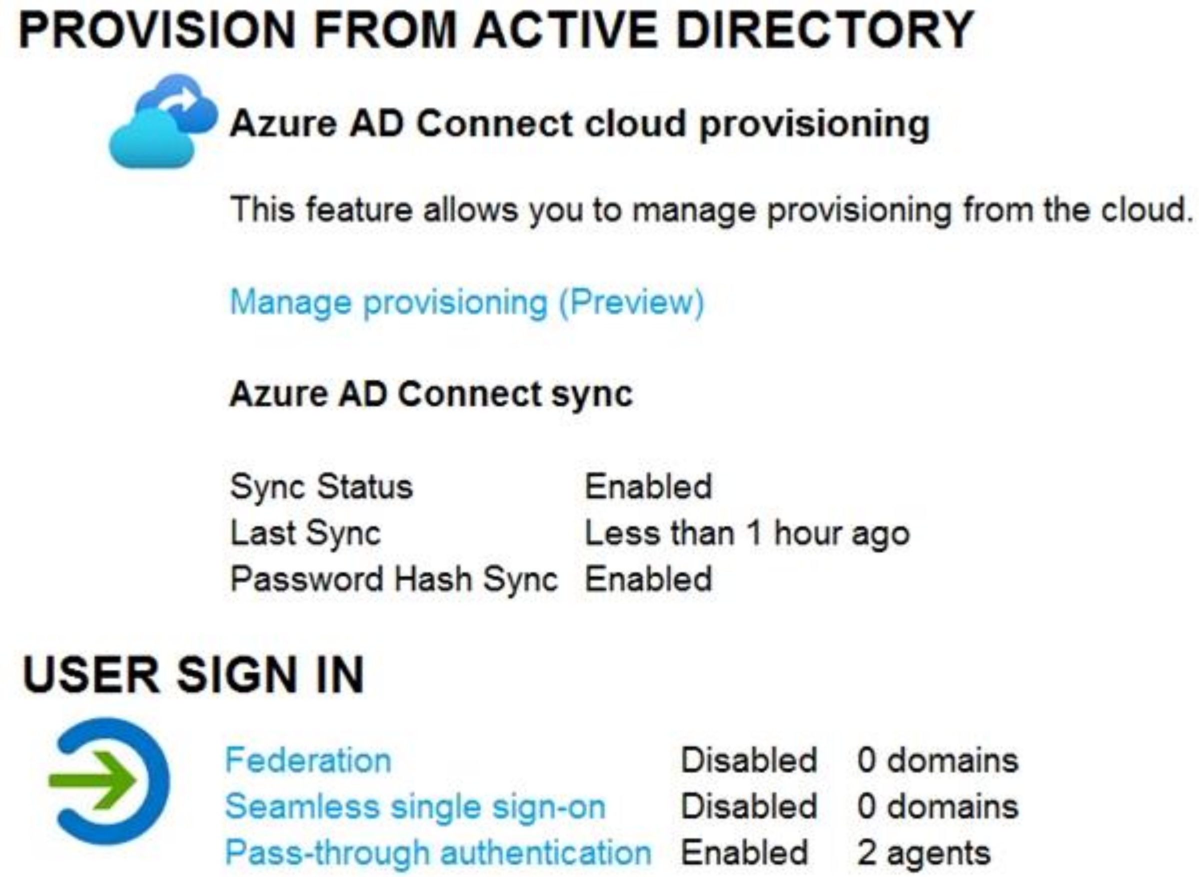
Your network contains an on-premises Active Directory domain that syncs to an Azure Active Directory (Azure AD) tenant. The tenant contains the users shown in the following table.



Name	Type	Directory synced
User1	User	No
User2	User	Yes
User3	Guest	No

All the users work remotely.

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



PROVISION FROM ACTIVE DIRECTORY

Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

Manage provisioning (Preview)

Azure AD Connect sync

Sync Status	Enabled
Last Sync	Less than 1 hour ago
Password Hash Sync	Enabled

USER SIGN IN

Federation	Disabled	0 domains
Seamless single sign-on	Disabled	0 domains
Pass-through authentication	Enabled	2 agents

Connectivity from the on-premises domain to the internet is lost.

Which users can sign in to Azure AD?

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

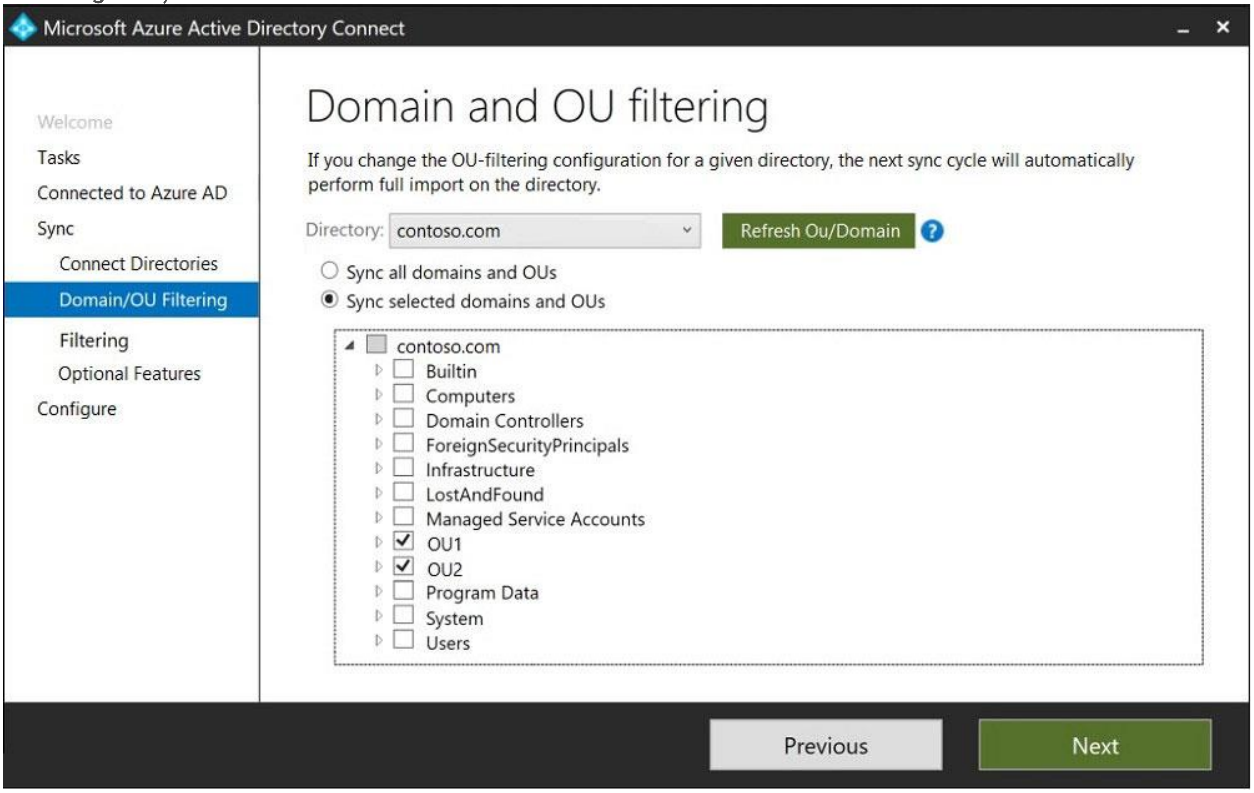
Question #19

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.)



Domain and OU filtering

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

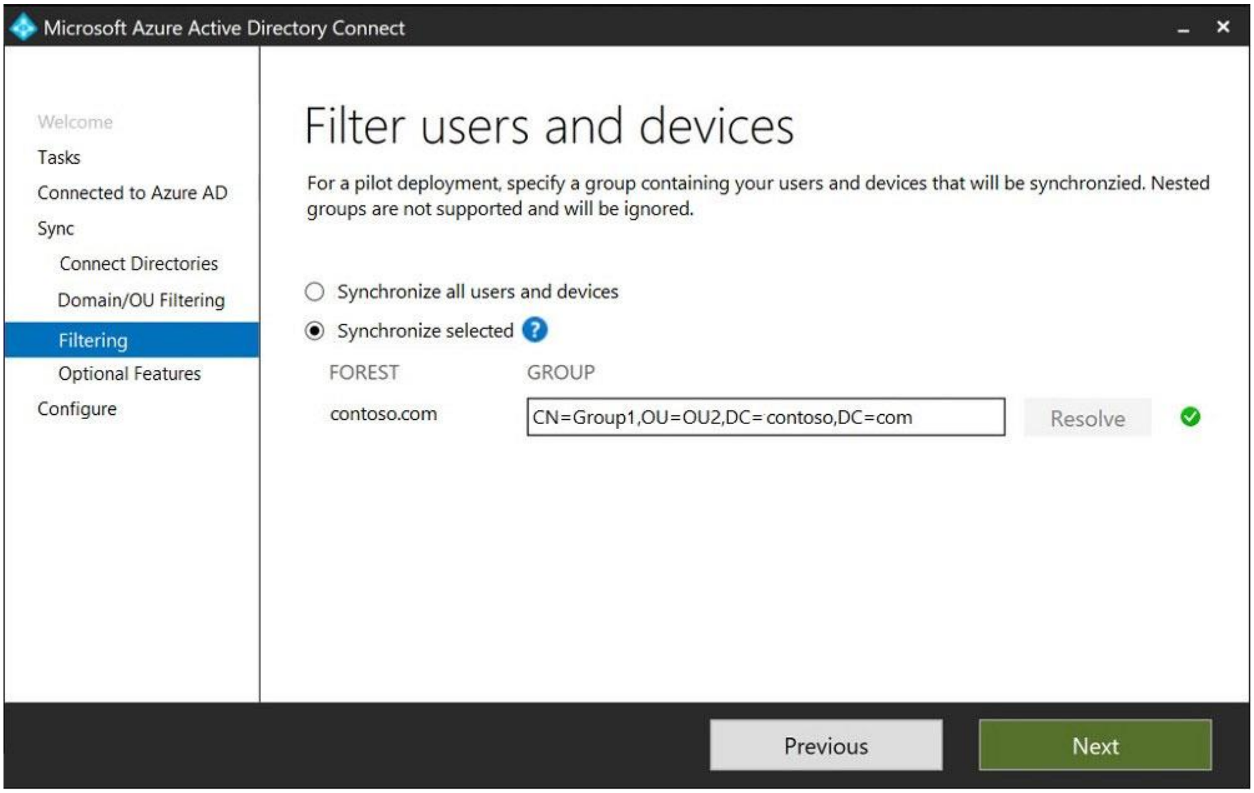
Directory: contoso.com

○ Sync all domains and OUs

● Sync selected domains and OUs

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

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



Filter users and devices

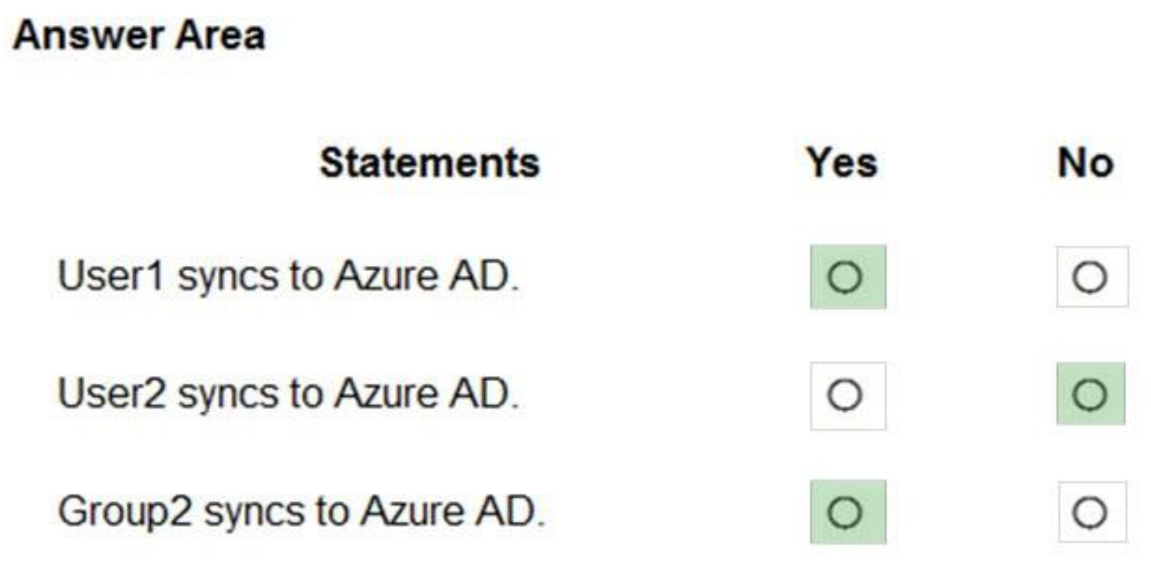
For a pilot deployment, specify a group containing your users and devices that will be synchronzied. Nested groups are not supported and will be ignored.

○ Synchronize all users and devices

● Synchronize selected

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

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



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.

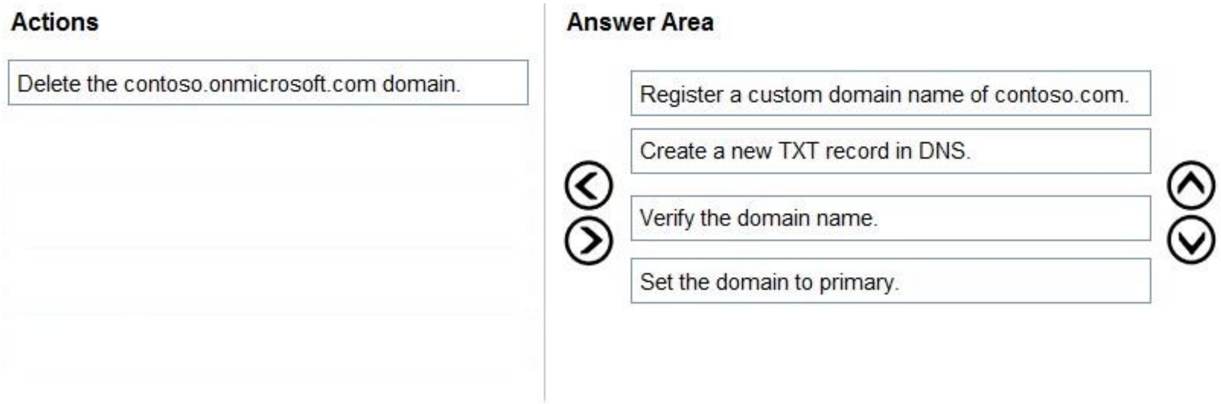
Question #20

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
- Question #21*Topic 1*

Question #21

DRAG DROP -
You have a new Microsoft 365 tenant that uses a domain name of contoso.onmicrosoft.com.
You register the name contoso.com with a domain registrar.
You need to use contoso.com as the default domain name for new Microsoft 365 users.
Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.
Select and Place:



Actions

Delete the contoso.onmicrosoft.com domain.

Answer Area

Register a custom domain name of contoso.com.

Create a new TXT record in DNS.

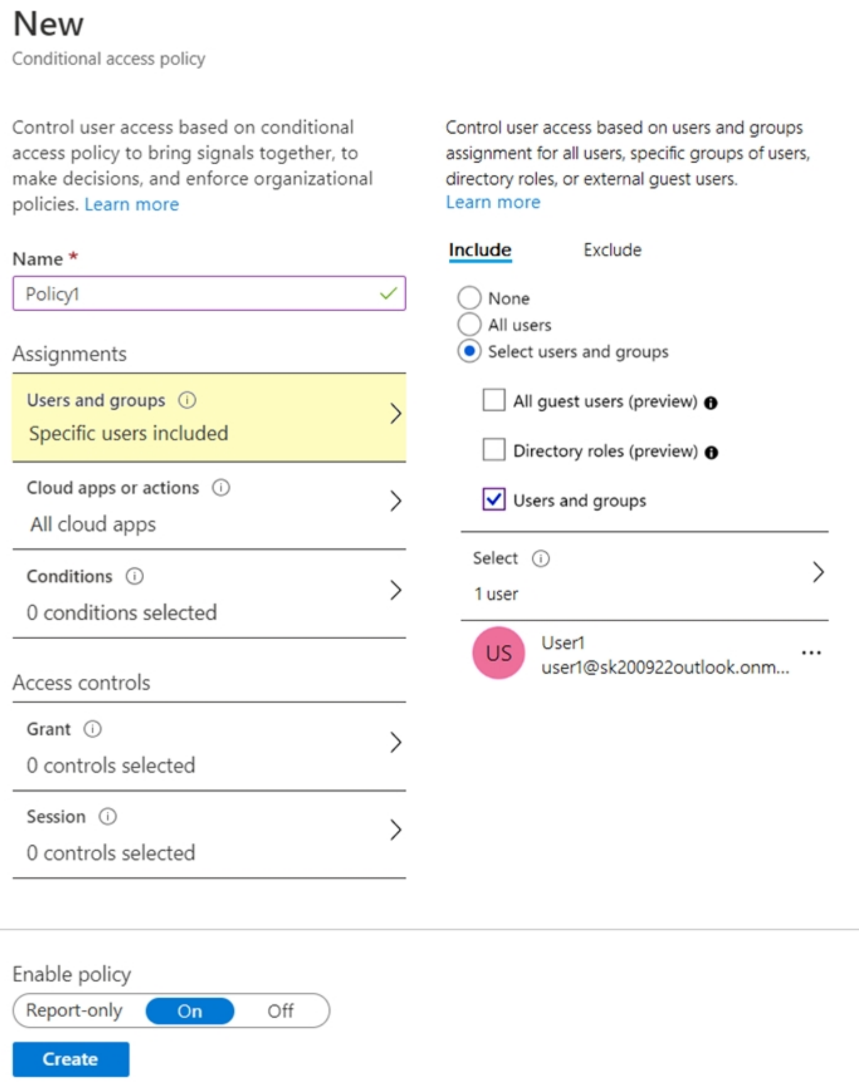
Verify the domain name.

Set the domain to primary.

Question #22

HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant that has Security defaults disabled.
You are creating a conditional access policy as shown in the following exhibit.



New

Conditional access policy

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

Policy1

Assignments

Users and groups ⓘ
Specific users included

Cloud apps or actions ⓘ
All cloud apps

Conditions ⓘ
0 conditions selected

Access controls

Grant ⓘ
0 controls selected

Session ⓘ
0 controls selected

Control user access based on users and groups assignment for all users, specific groups of users, directory roles, or external guest users.
Learn more

Include | Exclude

○ None
○ All users
● Select users and groups

□ All guest users (preview)
□ Directory roles (preview)
☑ Users and groups

Select ⓘ
1 user

US User1
user1@sk200922outlook.onm...

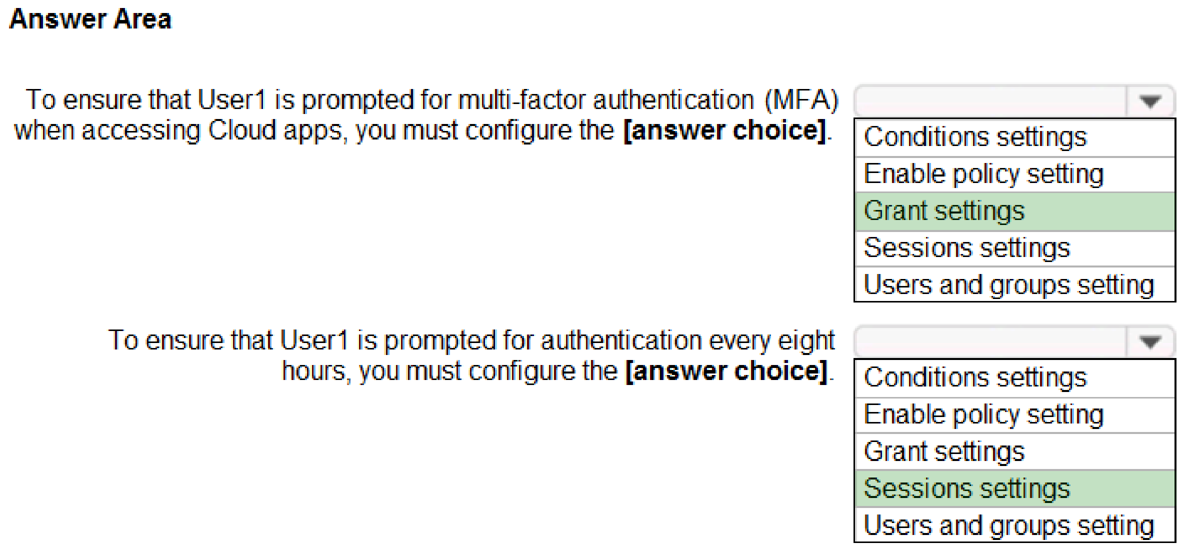
Enable policy

Report-only | **On** | Off

Create

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

Hot Area:



Answer Area

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

- Conditions settings
- Enable policy setting
- [✓ Grant settings]
- Sessions settings
- Users and groups setting

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

- Conditions settings
- Enable policy setting
- Grant settings
- [✓ Sessions settings]
- Users and groups setting

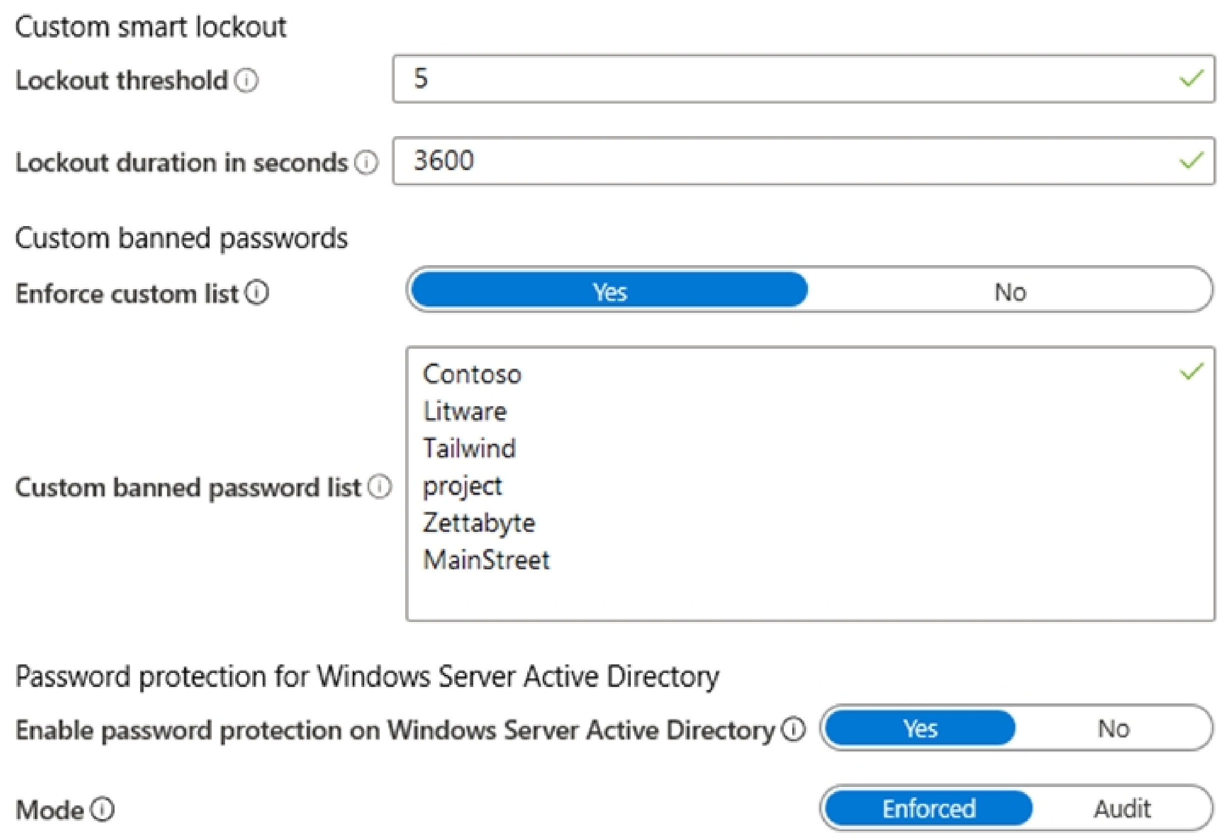
Question #23

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

Question #*24*

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



Custom smart lockout

Lockout threshold ⓘ: 5

Lockout duration in seconds ⓘ: 3600

Custom banned passwords

Enforce custom list ⓘ: [✓ Yes] No

Custom banned password list ⓘ:

Contoso
Litware
Tailwind
project
Zettabyte
MainStreet

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ: [✓ Yes] No

Mode ⓘ: [✓ Enforced] Audit

You are evaluating the following passwords:

✑ Pr0jectlitw@re
✑ T@ilw1nd
✑ C0nt0s0

Which passwords will be blocked?

- A. Pr0jectlitw@re and T@ilw1nd only
- B. C0nt0s0 only
- **C**. C0nt0s0, Pr0jectlitw@re, and T@ilw1nd
- D. C0nt0s0 and T@ilw1nd only
- E. C0nt0s0 and Pr0jectlitw@re only

Question #25

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**. Windows Hello
- D. SMS

Question #26

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.

Question #27

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

Question #28

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

Question #29

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

Question #30

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?

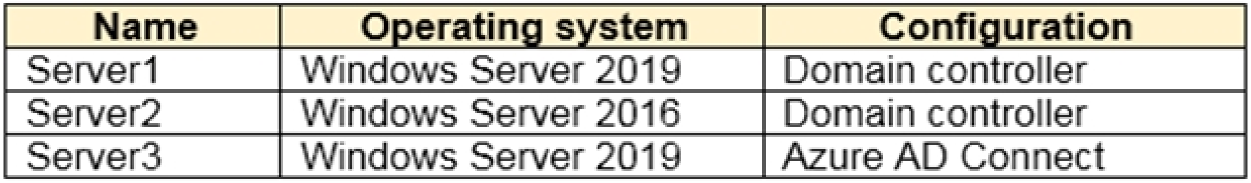
- A. a Microsoft Cloud App Security activity policy that has Microsoft Office 365 governance actions configured
- **B.** an Azure AD conditional access policy that has session controls configured
- C. an Azure AD conditional access policy that has client apps conditions configured
- D. a Microsoft Cloud App Security app discovery policy that has governance actions configured

Question #31

You have an Azure Active Directory (Azure AD) tenant that syncs to an Active Directory domain.
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

Question #32
You have a Microsoft 365 tenant.
The Azure Active Directory (Azure AD) tenant syncs to 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

Question #33

DRAG DROP -

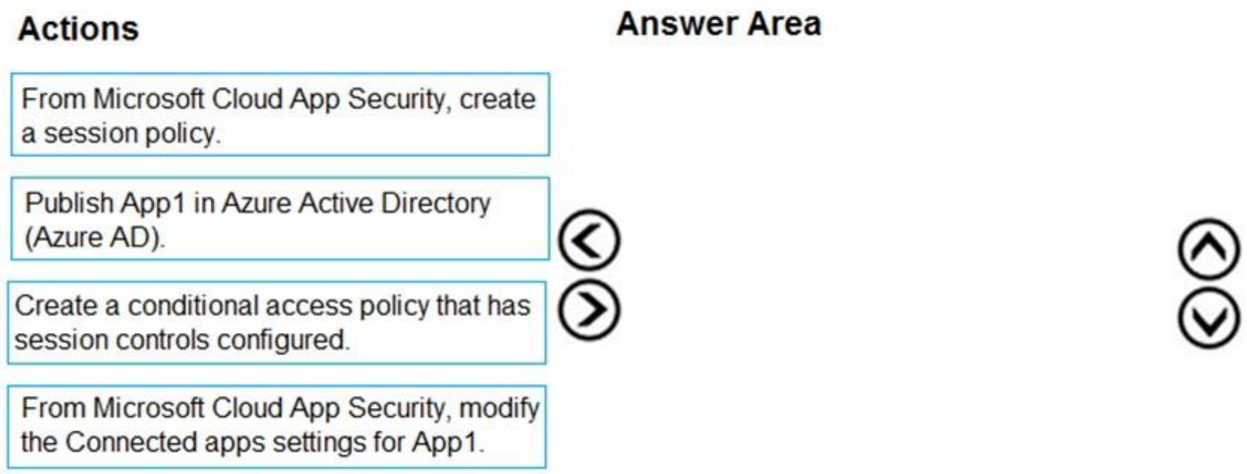
You have a Microsoft 365 E5 tenant.

You purchase a cloud app named App1.

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

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

Select and Place:



Actions

- From Microsoft Cloud App Security, create a session policy.
- Publish App1 in Azure Active Directory (Azure AD).
- Create a conditional access policy that has session controls configured.
- From Microsoft Cloud App Security, modify the Connected apps settings for App1.

Answer Area

1) publish app

2) create a conditional access policy that has session controls - this begins the process for
3) From MCAS create a session policy

4) from MCAS modify the connected apps settings

Question #34

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

Question #35

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

You need to configure the fraud alert settings.

Question #36

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
- You need to configure the fraud alert settings.

Question #37

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
- You need to configure the fraud alert settings.

Question #38

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.

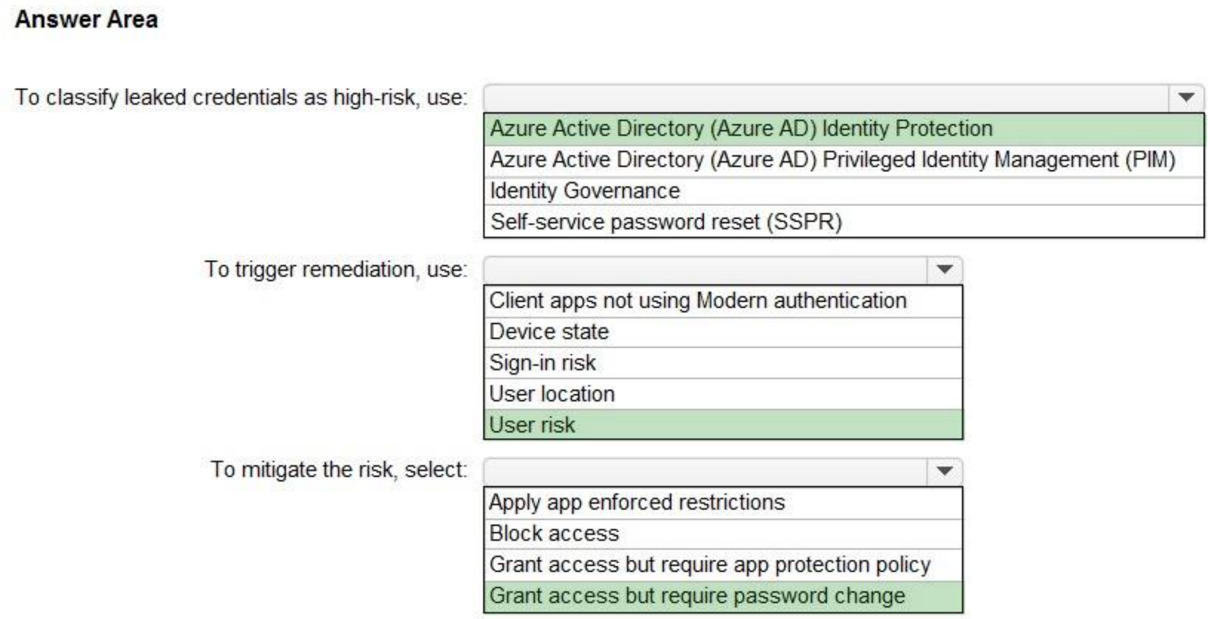
✑ Flag the sign-ins as a high-risk event.

✑ 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]

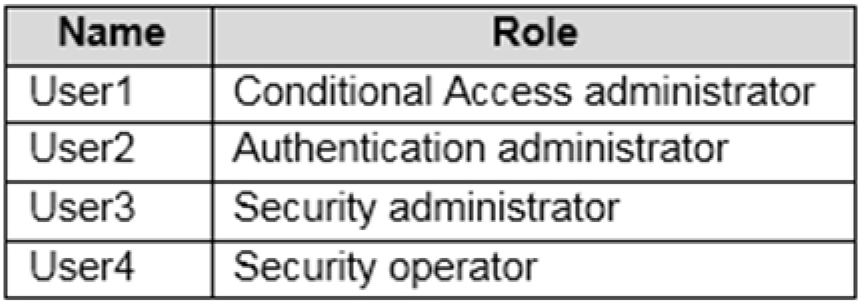
To mitigate the risk, select:

Apply app enforced restrictions
Block access
Grant access but require app protection policy
[✓ Grant access but require password change]

Question #39

HOTSPOT -

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



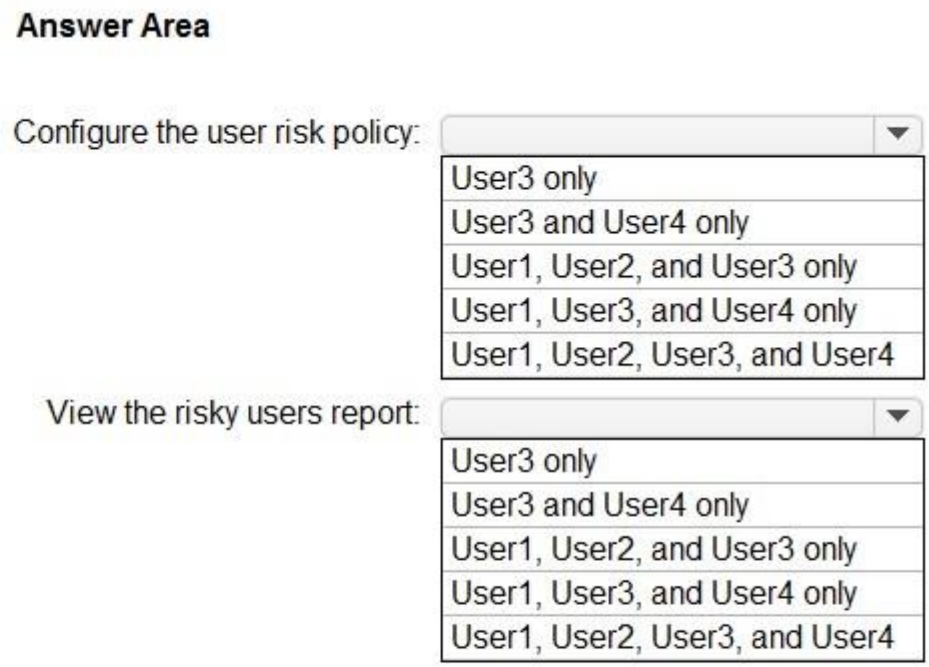
Name	Role
User1	Conditional Access administrator
User2	Authentication administrator
User3	Security administrator
User4	Security operator

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

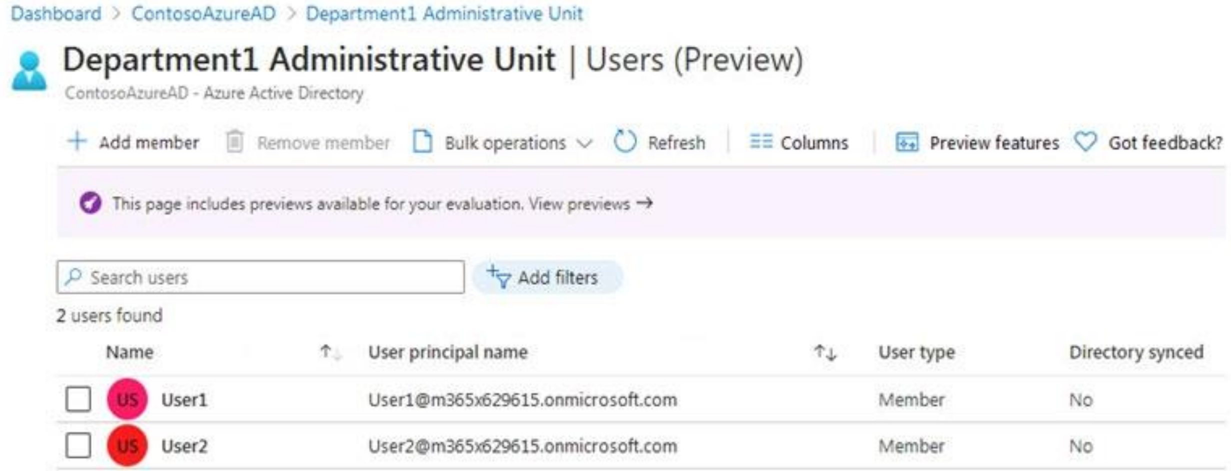
- Configure the user risk policy: User3 only
- View the risky users report: user3 and user4 only

Question #40

HOTSPOT -

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

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



Department1 Administrative Unit | Users (Preview)

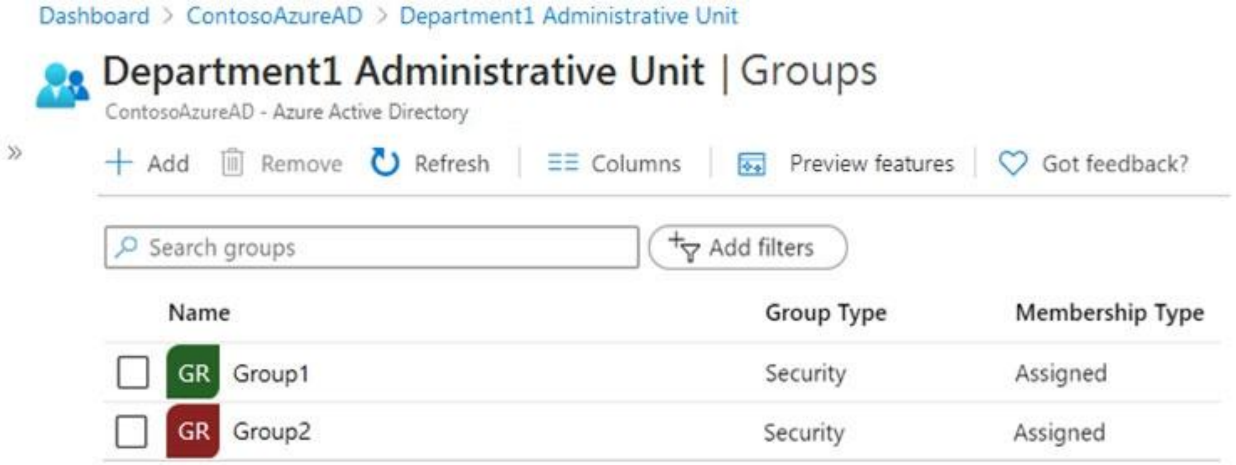
ContosoAzureAD - Azure Active Directory

This page includes previews available for your evaluation. View previews →

2 users found

Name	User principal name	User type	Directory synced
User1	User1@m365x629615.onmicrosoft.com	Member	No
User2	User2@m365x629615.onmicrosoft.com	Member	No

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

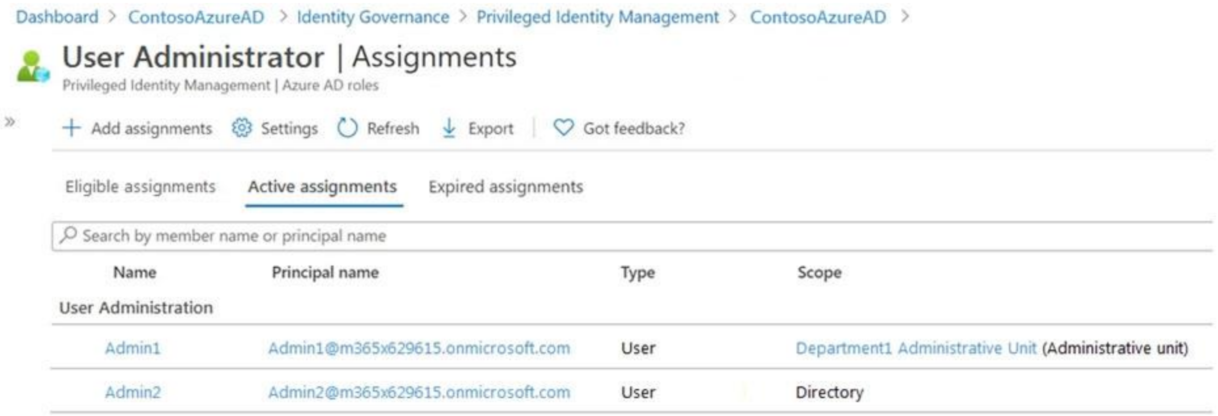


Department1 Administrative Unit | Groups

ContosoAzureAD - Azure Active Directory

Name	Group Type	Membership Type
Group1	Security	Assigned
Group2	Security	Assigned

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



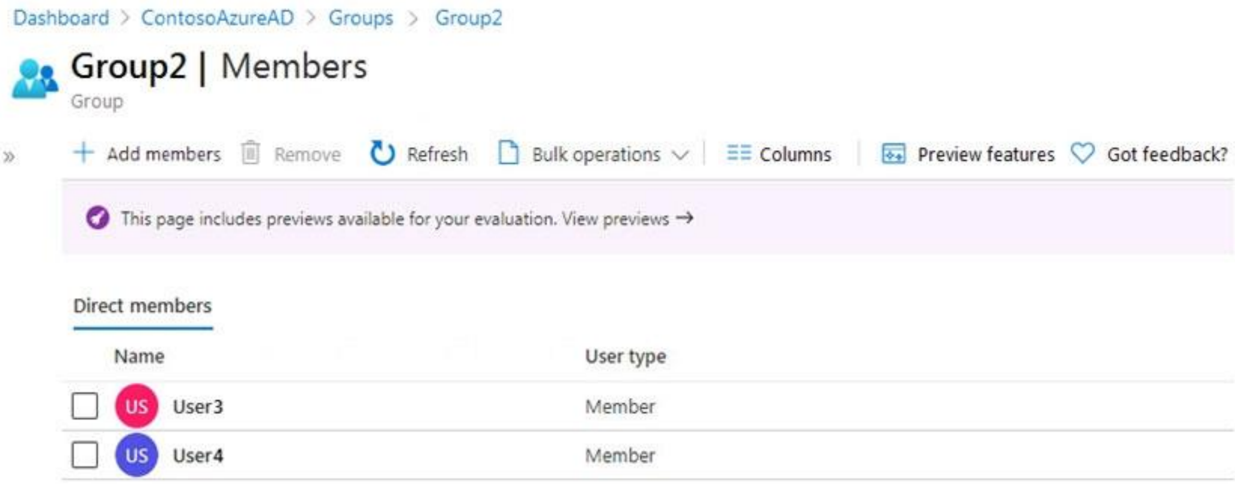
Dashboard > ContosoAzureAD > Identity Governance > Privileged Identity Management > ContosoAzureAD >

User Administrator | Assignments

Privileged Identity Management | Azure AD roles

Name	Principal name	Type	Scope
User Administration			
Admin1	Admin1@m365x629615.onmicrosoft.com	User	Department1 Administrative Unit (Administrative unit)
Admin2	Admin2@m365x629615.onmicrosoft.com	User	Directory

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



Dashboard > ContosoAzureAD > Groups > Group2

Group2 | Members

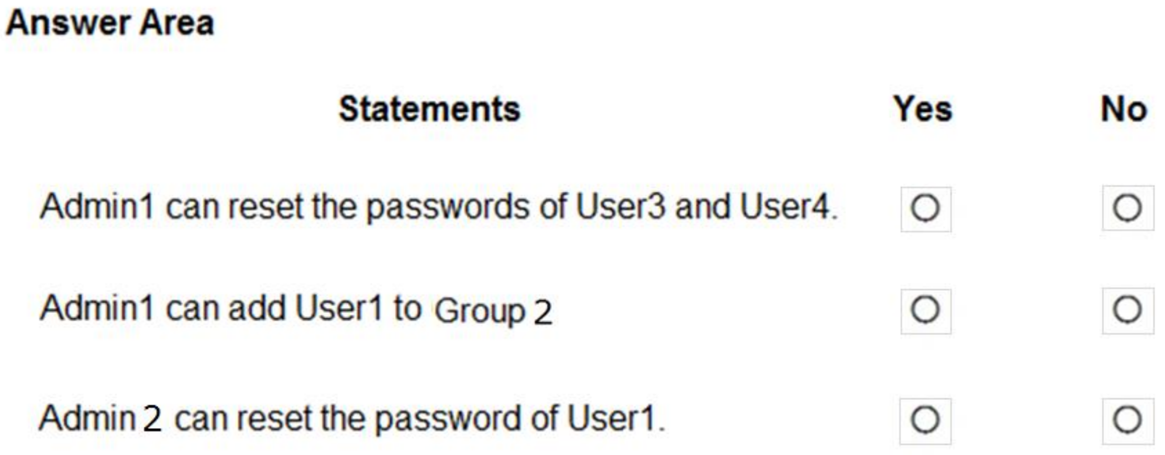
Group

This page includes previews available for your evaluation. View previews →

Direct members

Name	User type
□ US User3	Member
□ US User4	Member

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



Answer Area

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

The answers: **Yes, no, no.** NO YES YES

Question #41

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:

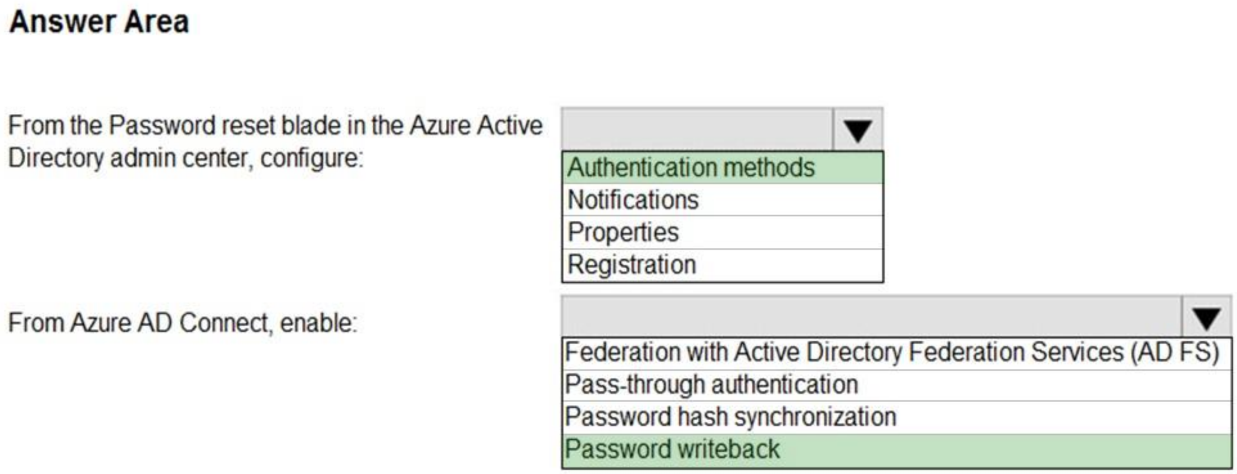
✑ When users reset their password, they must be prompted to respond to a mobile app notification or answer three predefined security questions.

✑ 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:

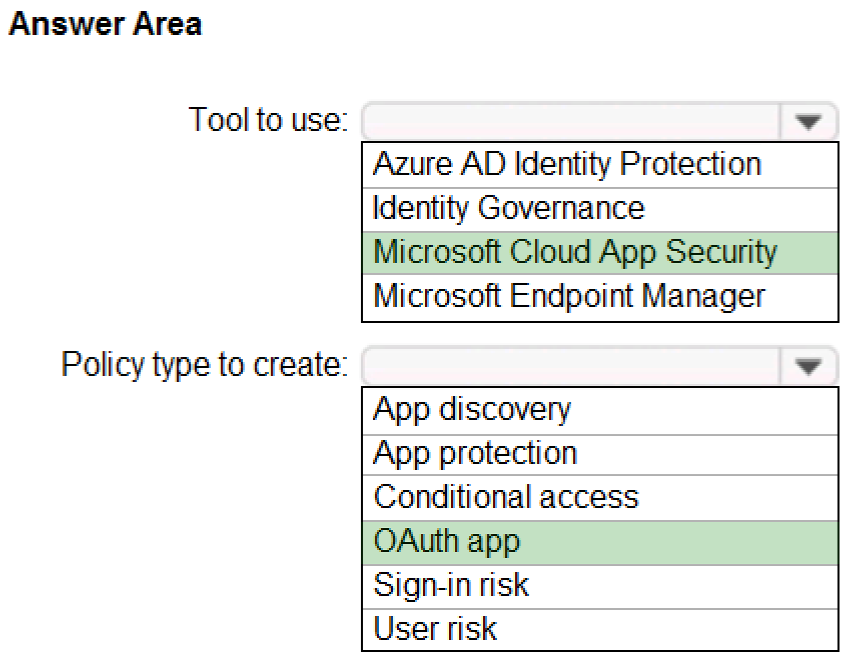
▼
- [✓ Authentication methods]
- Notifications
- Properties
- Registration

From Azure AD Connect, enable:

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

Question #42

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 usersג€™ 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

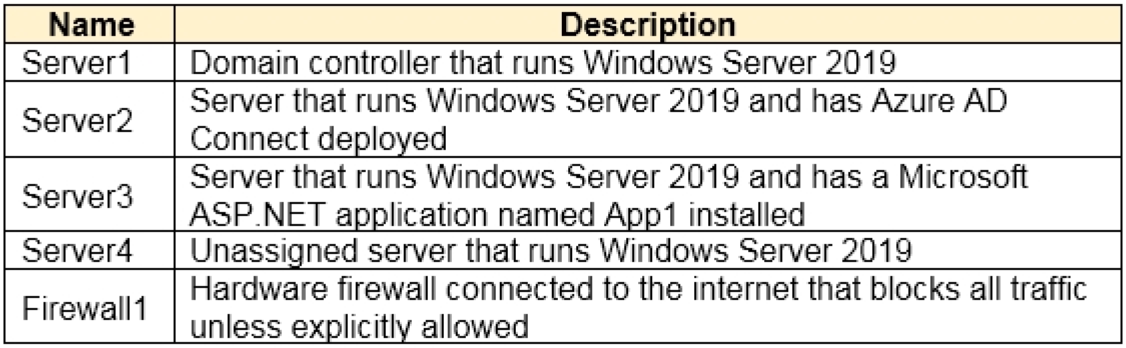
Question #43

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

Question #44

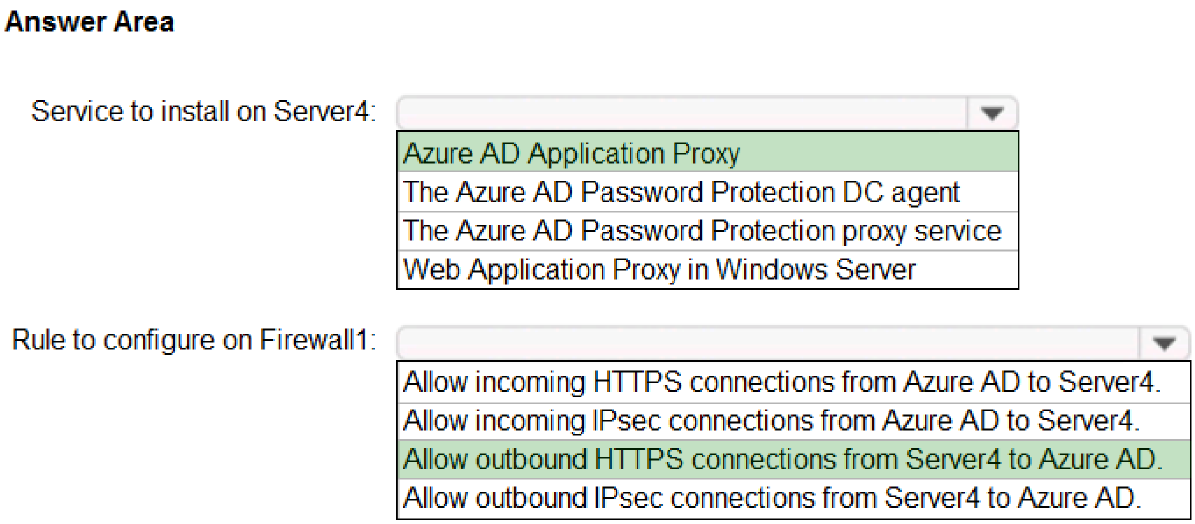
HOTSPOT -
You have an on-premises datacenter that contains the hosts shown in the following table.



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

You have an Azure Active Directory (Azure AD) tenant that syncs to the Active Directory forest.
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 Server 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

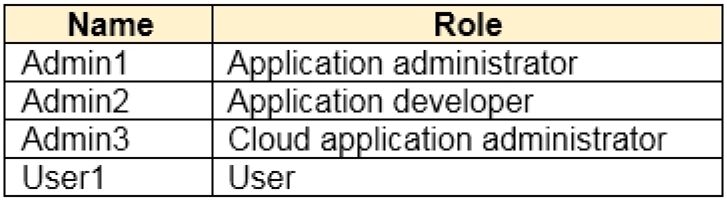
Rule to configure on Firewall1:

- 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.

Question #45

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

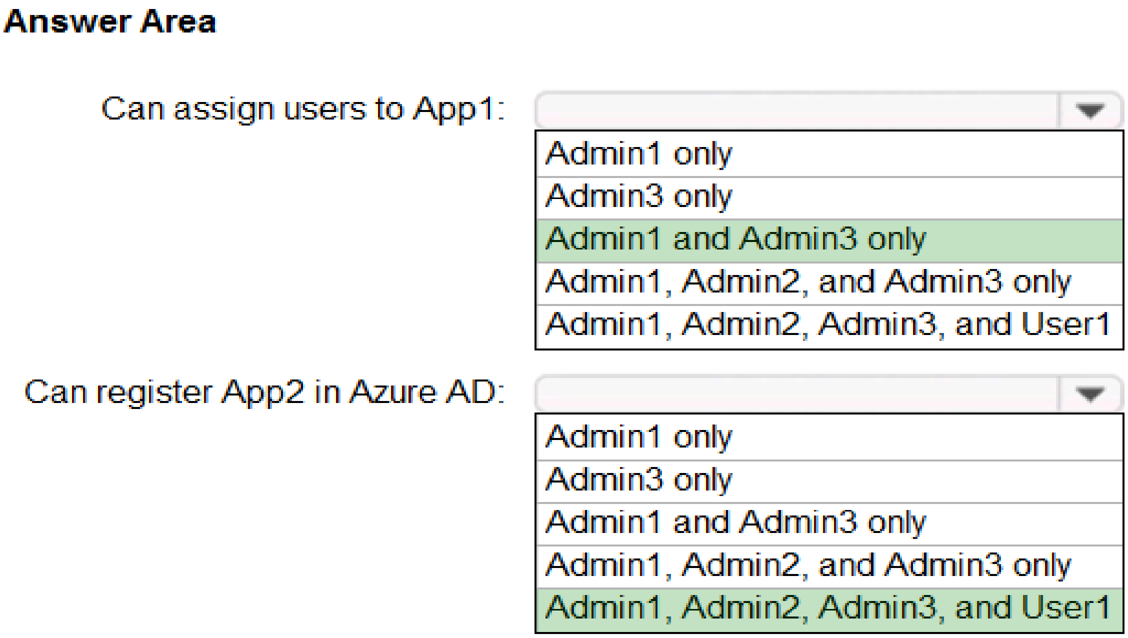
You purchase two cloud apps named App1 and App2. The global administrator registers App1 in Azure AD.

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

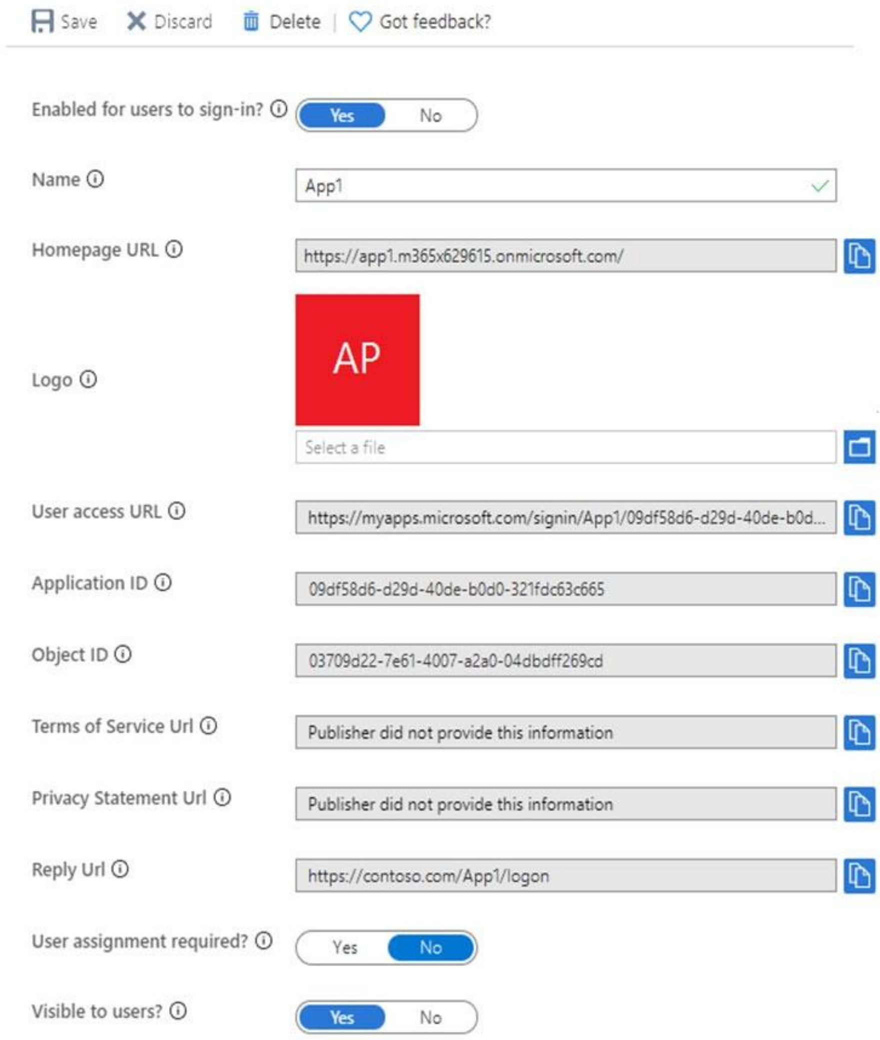
Can register App2 in Azure AD:

- Admin1 only
- Admin3 only
- Admin1 and Admin3 only
- Admin1, Admin2, and Admin3 only
- [✓ Admin1, Admin2, Admin3, and User1]

Question #46

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.



Enabled for users to sign-in? [✓ Yes] No

Name: App1

Homepage URL: https://app1.m365x629615.onmicrosoft.com/

Logo

User access URL: https://myapps.microsoft.com/signin/App1/09df58d6-d29d-40de-b0d...

Application ID: 09df58d6-d29d-40de-b0d0-321fdc63c665

Object ID: 03709d22-7e61-4007-a2a0-04dbdff269cd

Terms of Service Url: Publisher did not provide this information

Privacy Statement Url: Publisher did not provide this information

Reply Url: https://contoso.com/App1/logon

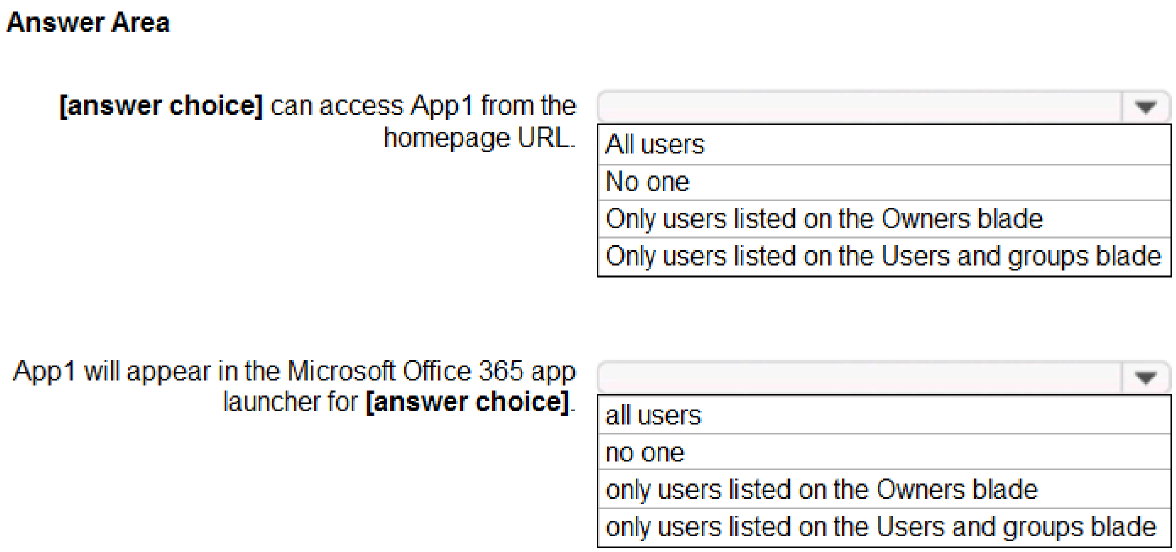
User assignment required? Yes [✓ No]

Visible to users? [✓ Yes] 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

[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

The answers are:

- **[All Users]** can access App1 from the homepage URL

- App1 will appear in the Microsoft office 365 app launcher for **[only users listed on the Users and groups blade]**

Question #47

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.

Question #48

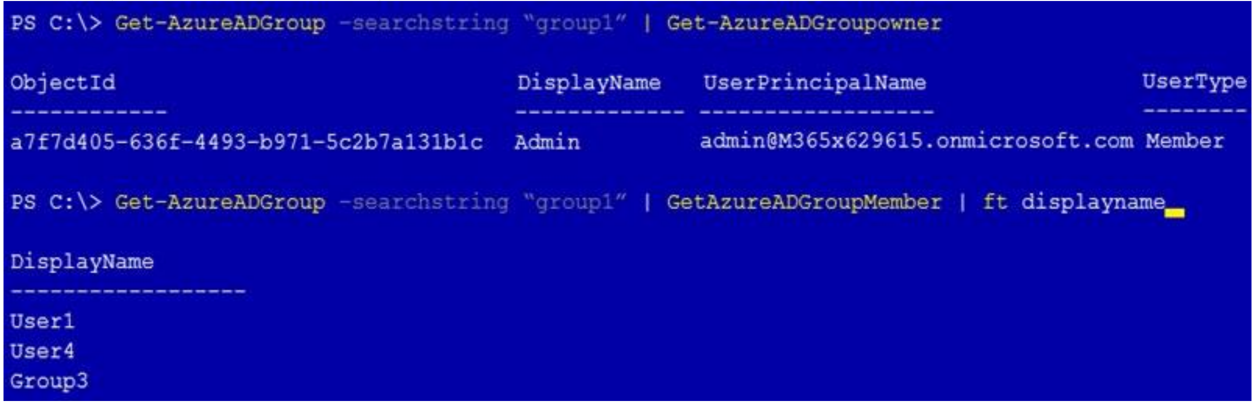
You have an Azure Active Directory (Azure AD) tenant.
For the tenant, Users can register applications is set to No.
A user named Admin1 must deploy a new cloud app named App1.
You need to ensure that Admin1 can register App1 in Azure AD. The solution must use the principle of least privilege.
Which role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

Question #49

HOTSPOT -

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



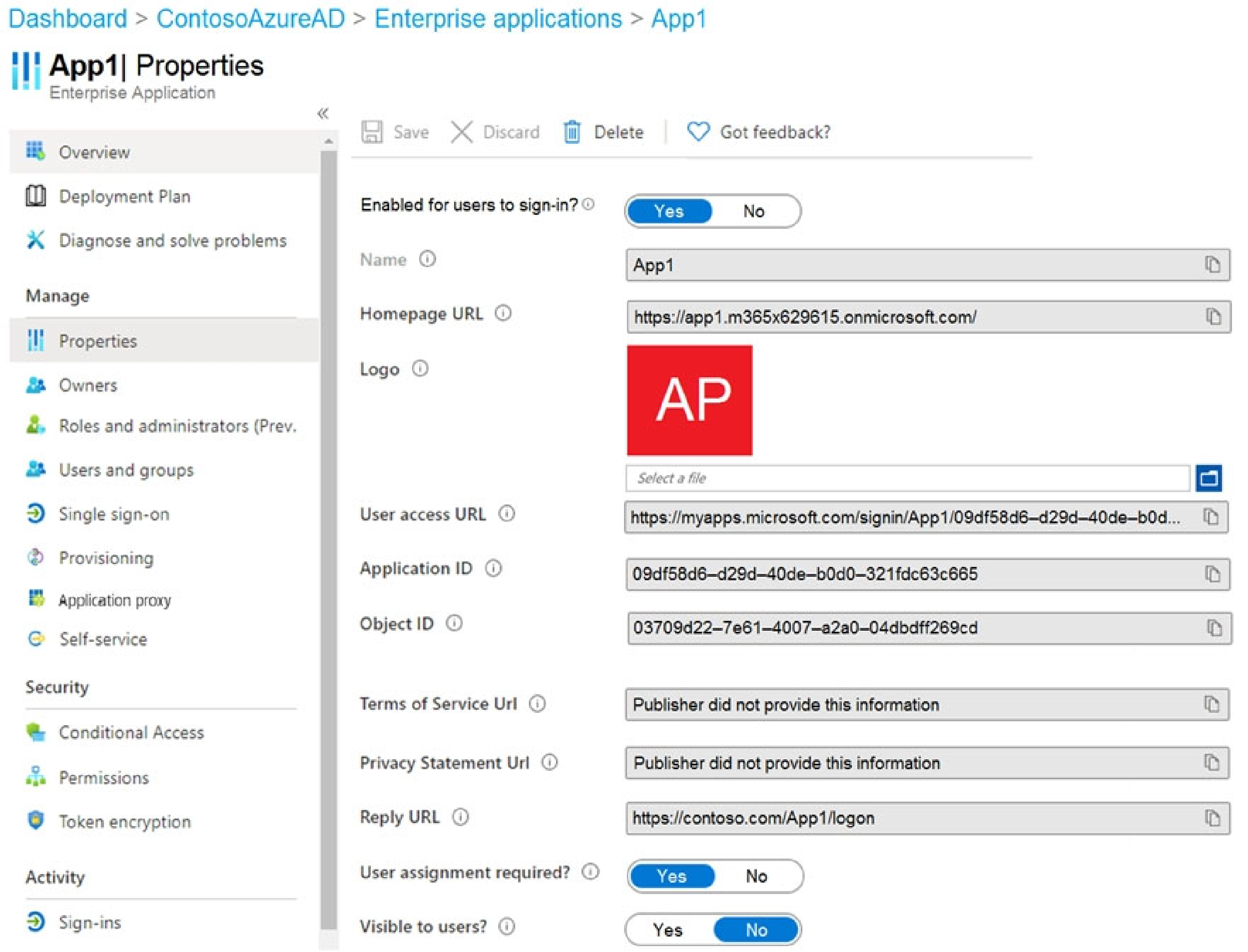
```
PS C:\> Get-AzureADGroup -searchstring "group1" | Get-AzureADGroupowner

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.)



Dashboard > ContosoAzureAD > Enterprise applications > App1

App1| Properties

Enterprise Application

Enabled for users to sign-in? [✓ Yes] No

Name: App1

Homepage URL: https://app1.m365x629615.onmicrosoft.com/

Logo

User access URL: https://myapps.microsoft.com/signin/App1/09df58d6–d29d–40de–b0d...

Application ID: 09df58d6–d29d–40de–b0d0–321fdc63c665

Object ID: 03709d22–7e61–4007–a2a0–04dbdff269cd

Terms of Service Url: Publisher did not provide this information

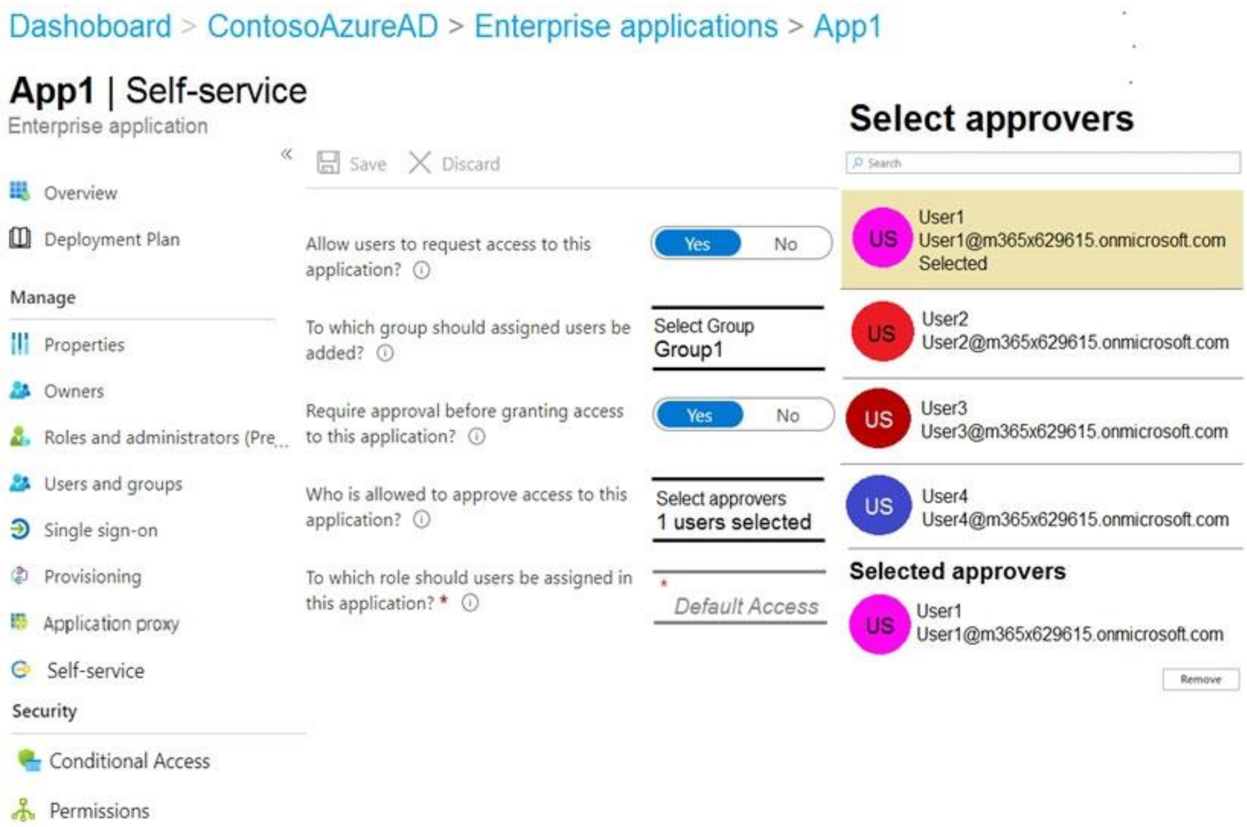
Privacy Statement Url: Publisher did not provide this information

Reply URL: https://contoso.com/App1/logon

User assignment required? [✓ Yes] No

Visible to users? Yes [✓ No]

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



Dashoboard > ContosoAzureAD > Enterprise applications > App1

App1 | Self-service

Enterprise application

Allow users to request access to this application? ⓘ — Yes | No (Yes selected)

To which group should assigned users be added? ⓘ — Select Group: Group1

Require approval before granting access to this application? ⓘ — Yes | No (Yes selected)

Who is allowed to approve access to this application? ⓘ — Select approvers: 1 users selected

To which role should users be assigned in this application? * ⓘ — * Default Access

Select approvers

US User1 User1@m365x629615.onmicrosoft.com Selected

US User2 User2@m365x629615.onmicrosoft.com

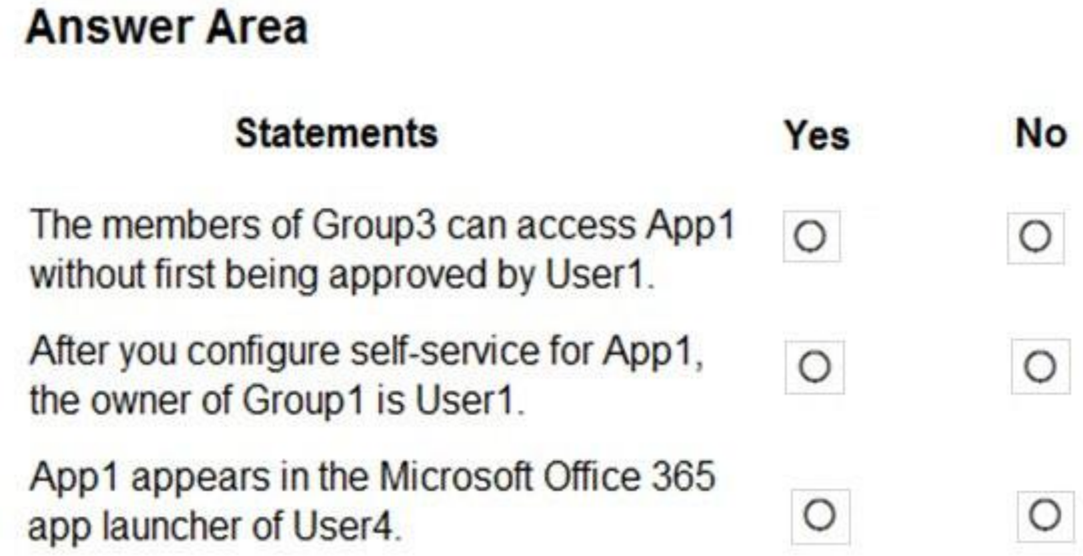
US User3 User3@m365x629615.onmicrosoft.com

US User4 User4@m365x629615.onmicrosoft.com

Selected approvers

US User1 User1@m365x629615.onmicrosoft.com

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



Answer Area

Statements	Yes	No
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.	○	○

The answers

- **No, yes, yes**   No No No

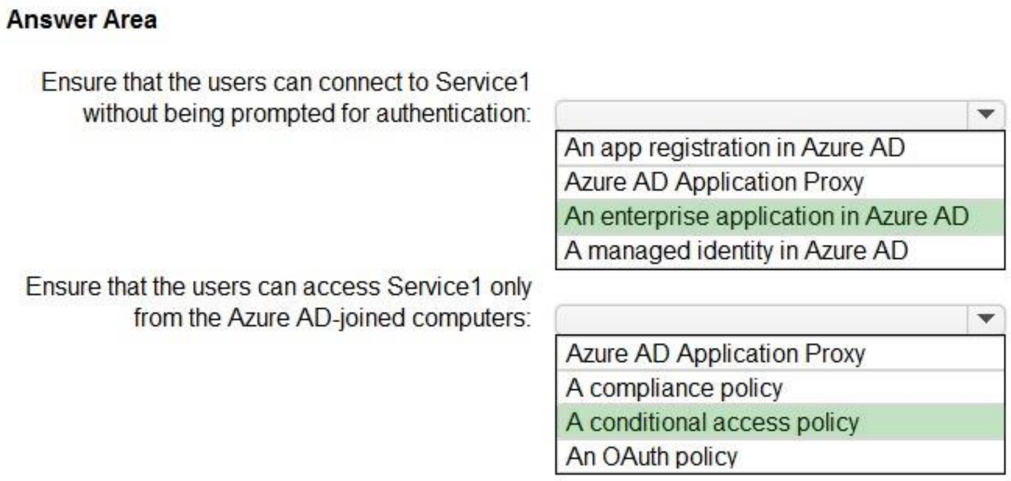
Question #50

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.

Question #51

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

Question #52
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?

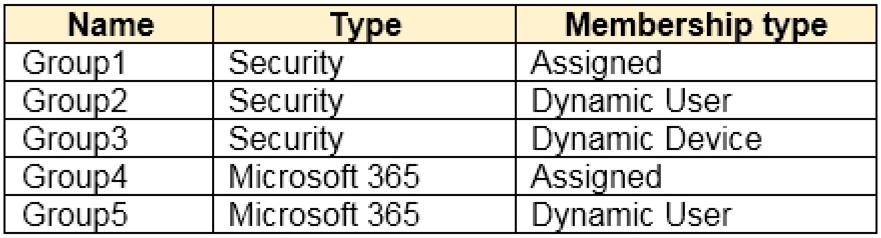
- **A.** Self-service
- B. Provisioning
- C. Application proxy
- D. Roles and administrators

Question #53

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

Question #54
You have an Azure Active Directory (Azure AD) tenant that contains the groups shown in the following table.



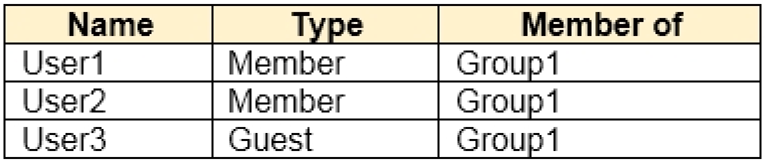
Name	Type	Membership type
Group1	Security	Assigned
Group2	Security	Dynamic User
Group3	Security	Dynamic Device
Group4	Microsoft 365	Assigned
Group5	Microsoft 365	Dynamic User

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

Question #55

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

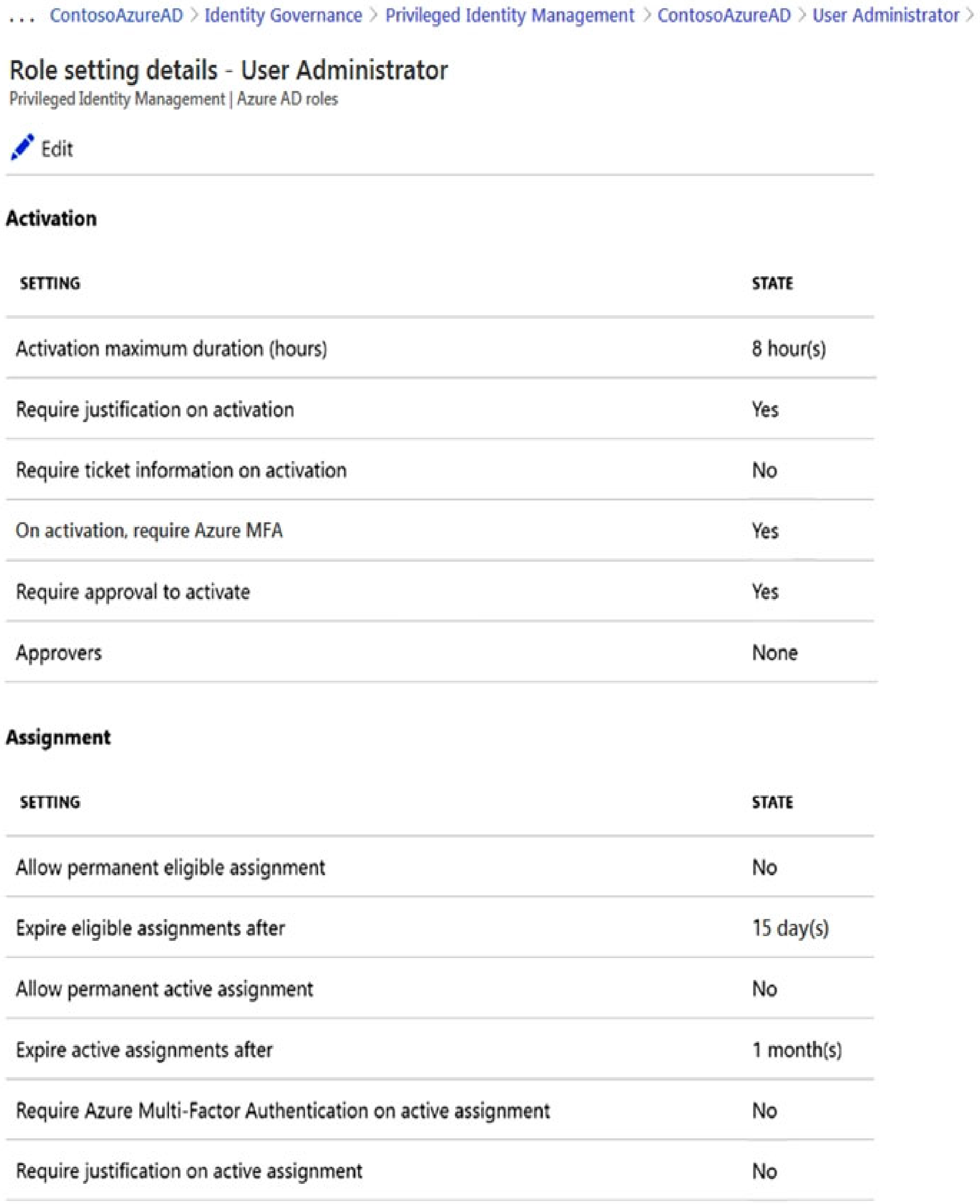
✑ Reviewers: Members (self)

Which users can perform access reviews for User3?

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

Question #56

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

Activation

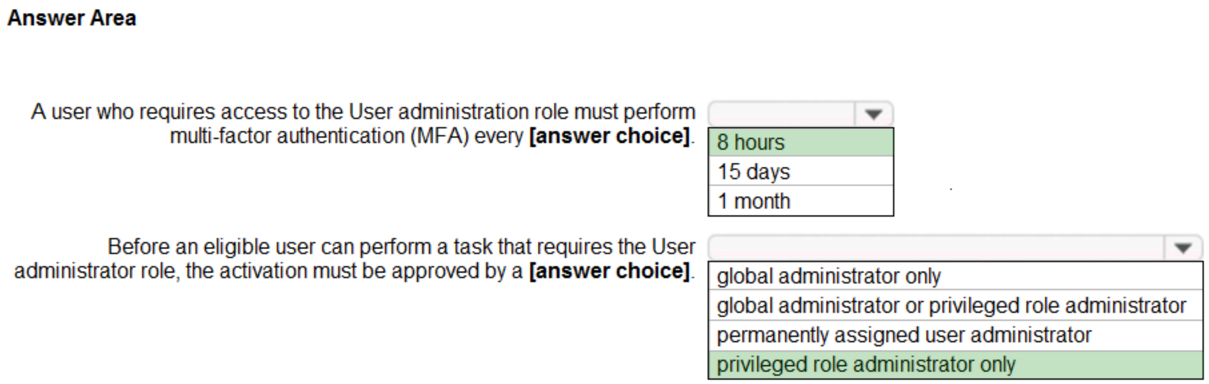
SETTING	STATE
Activation maximum duration (hours)	8 hour(s)
Require justification on activation	Yes
Require ticket information on activation	No
On activation, require Azure MFA	Yes
Require approval to activate	Yes
Approvers	None

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]**.

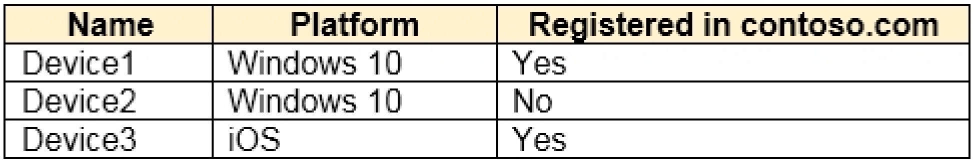
- [✓ 8 hours]
- 15 days
- 1 month

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]

Question #57

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.



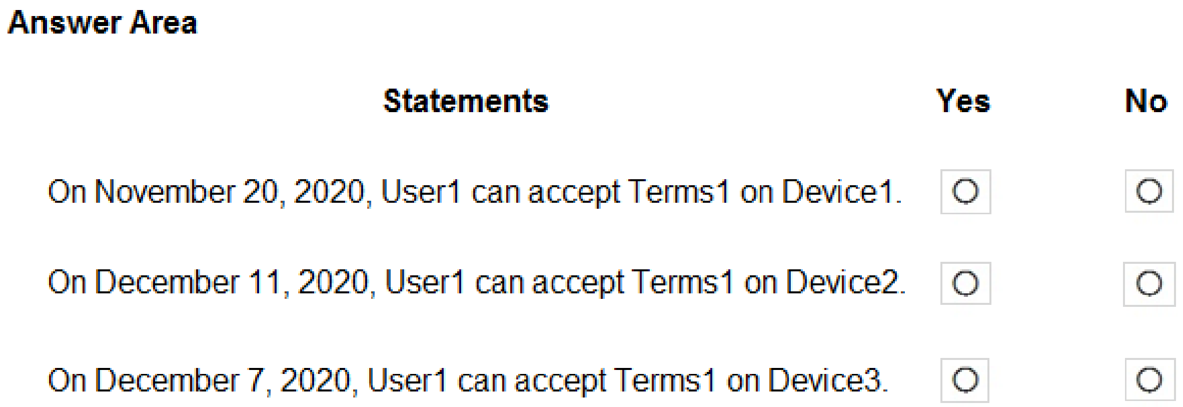
Name	Platform	Registered in contoso.com
Device1	Windows 10	Yes
Device2	Windows 10	No
Device3	iOS	Yes

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.	○	○

The answers: Yes, no, no YES YES NO

Question #58

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

Question #59

You have a Microsoft 365 tenant.

The Sign-ins activity report shows that an external contractor signed into 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

Question #60

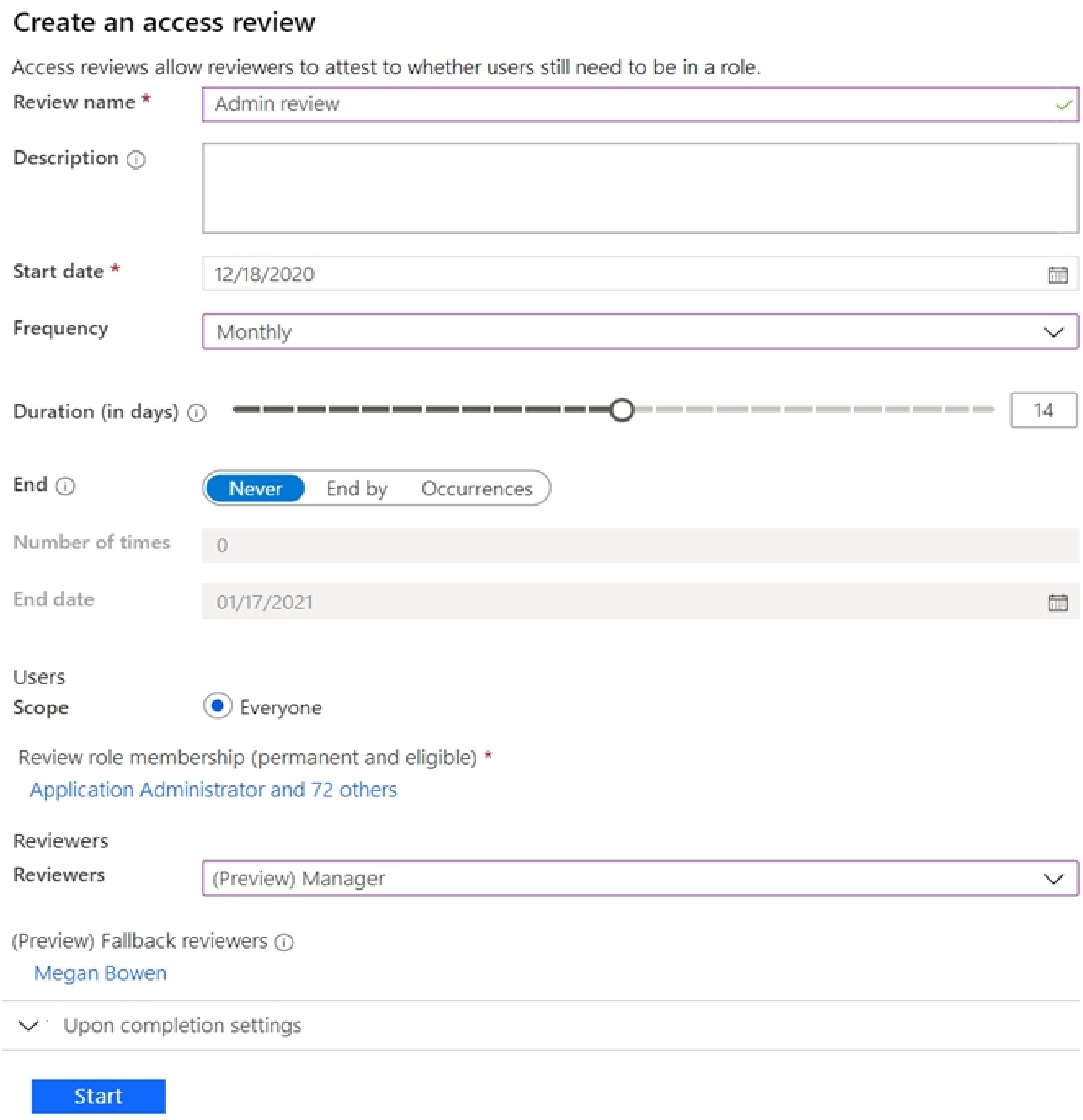
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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.)



Create an access review

Access reviews allow reviewers to attest to whether users still need to be in a role.

Review name * Admin review ✓

Description ⓘ

Start date * 12/18/2020

Frequency Monthly

Duration (in days) ⓘ 14

End ⓘ [✓ Never] End by Occurrences

Number of times 0

End date 01/17/2021

Users

Scope ● Everyone

Review role membership (permanent and eligible) *

Application Administrator and 72 others

Reviewers

Reviewers (Preview) Manager

(Preview) Fallback reviewers ⓘ

Megan Bowen

Upon completion settings

Start

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

Question #61

Solution: **You modify the properties of the IT administrator user accounts**.
Does this meet the goal?

- **A.** Yes
- B. No

Question #62

Solution: You set Reviewers to Member (self).
Does this meet the goal?

- A. Yes
- **B.** No

Question #63

Solution: You add each manager as a fallback reviewer.
Does this meet the goal?

- A. Yes
- **B**. No

Question #64

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.

Question #65

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**. Settings
- C. Terms of use
- D. Access reviews

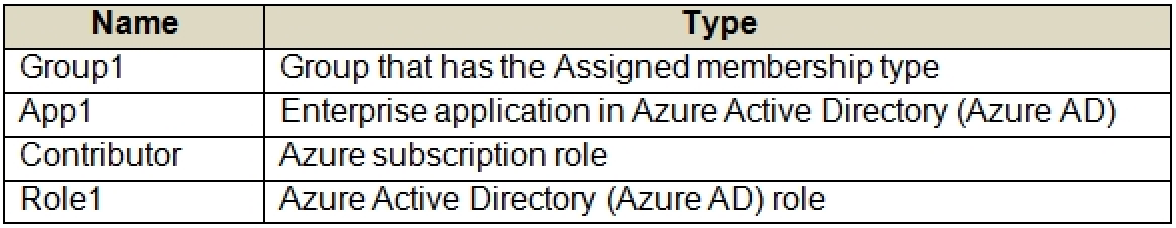
Question #66

You have an Azure Active Directory (Azure AD) 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

Question #67

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 (incorrect)
- D. Role1 and Contributor only

Explanation: you can assign access review to: - Applications - Teams and groups: All Microsoft 365 groups with guest users = (Guest users only) or : Select Teams + groups

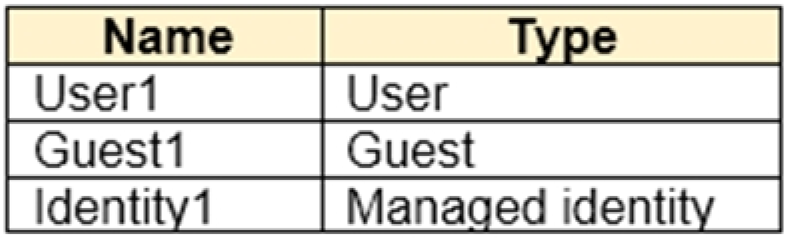
Question #68

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

Question #69

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

Question #70

HOTSPOT -

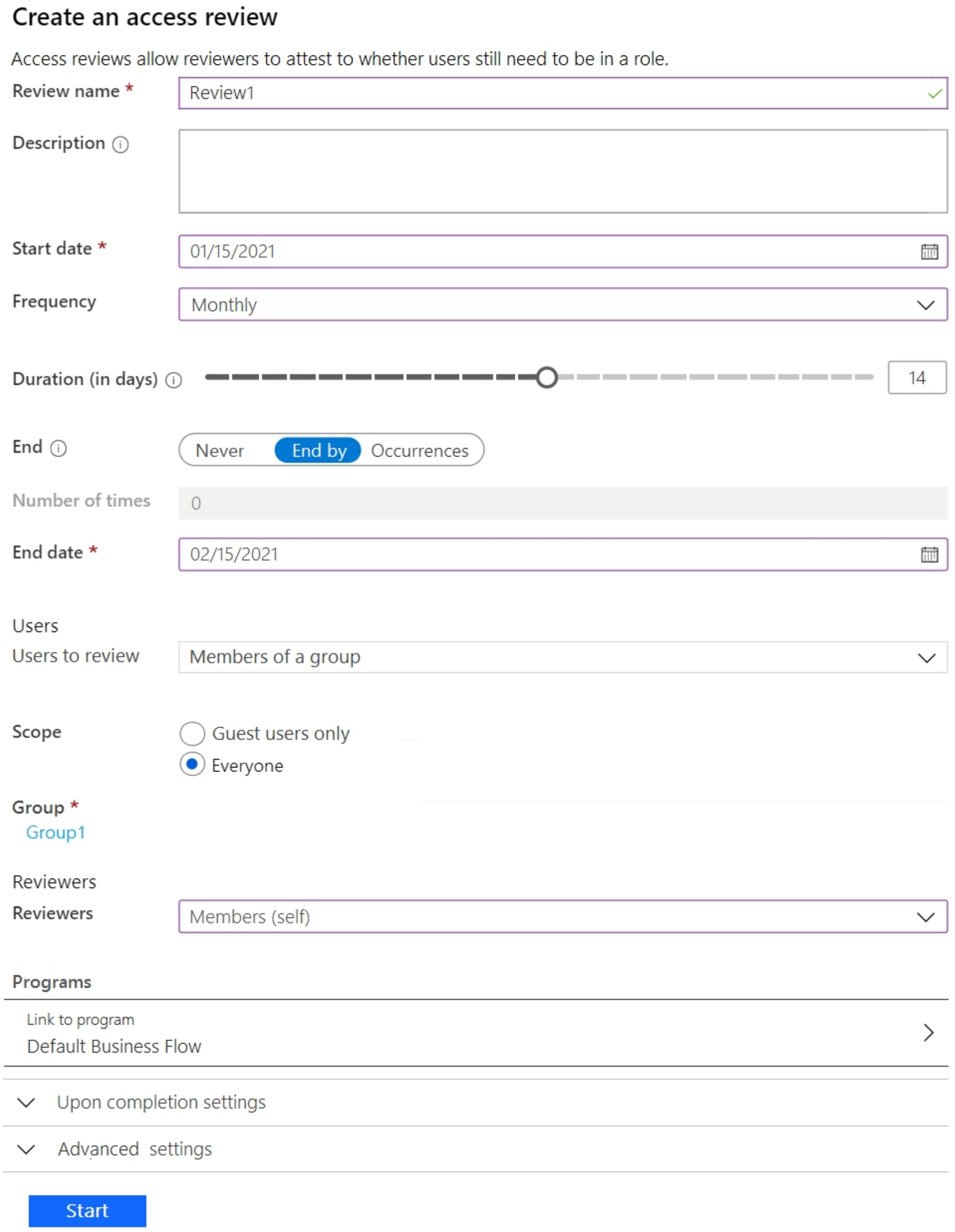
You have an Azure Active Directory (Azure AD) tenant that contains the following group:

➪ 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.)



Create an access review

Access reviews allow reviewers to attest to whether users still need to be in a role.

Review name * Review1 ✓

Description ⓘ

Start date * 01/15/2021

Frequency Monthly

Duration (in days) ⓘ 14

End ⓘ Never [✓ End by] Occurrences

Number of times 0

End date * 02/15/2021

Users

Users to review Members of a group

Scope

○ Guest users only

● Everyone

Group *

Group1

Reviewers

Reviewers Members (self)

Programs

Link to program

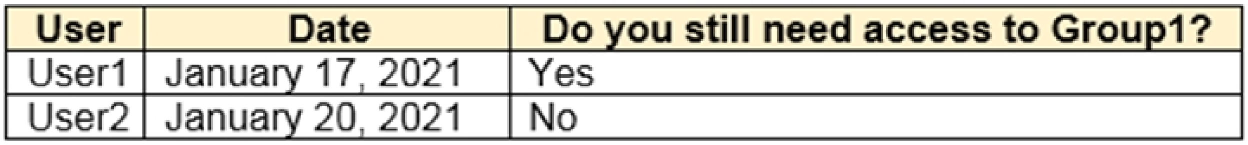
Default Business Flow

Upon completion settings

Advanced settings

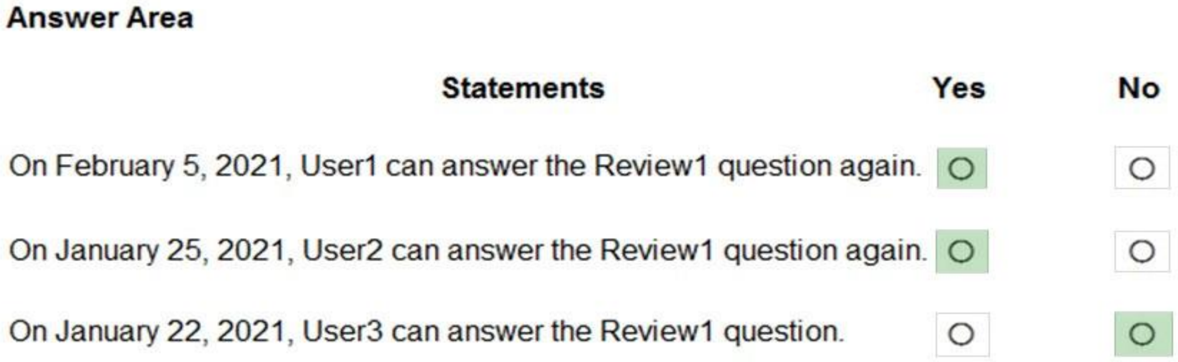
Start

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:

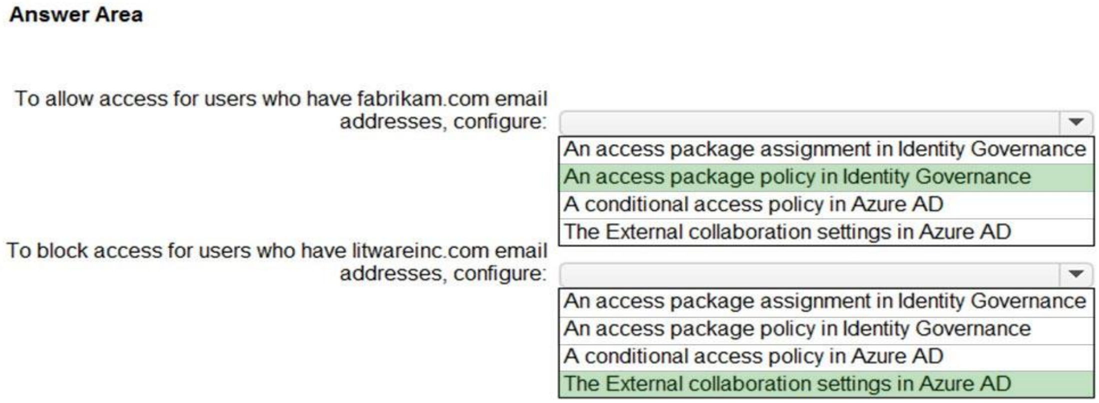


Answer Area

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.	○	[✓ ○]

Question #71

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]

Question #72

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 an Azure Sentinel data connector.
- B. Configure the Notify settings in Azure AD Identity Protection.
- C. Create an Azure Sentinel playbook.
- D. Modify the Diagnostics settings in Azure AD.

CASE STUDY

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 users shown in the following table.

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.
Requirement. 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 departmentג€™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 usersג€™ identity was compromised.

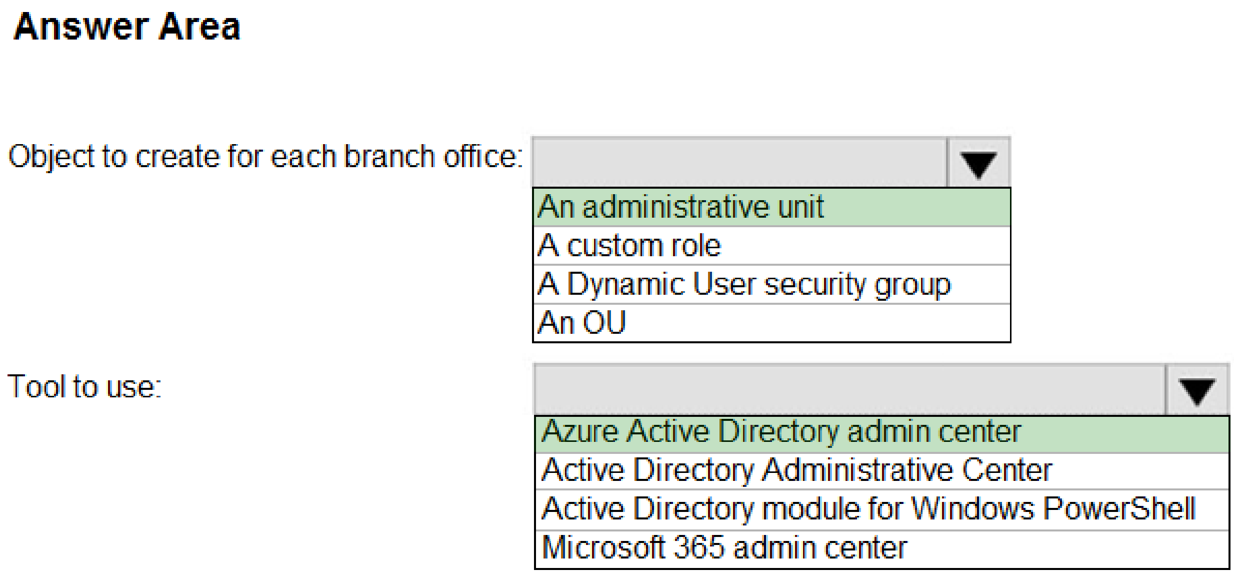
Question #73
You need to sync the ADatum users.

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.

Question #74

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:



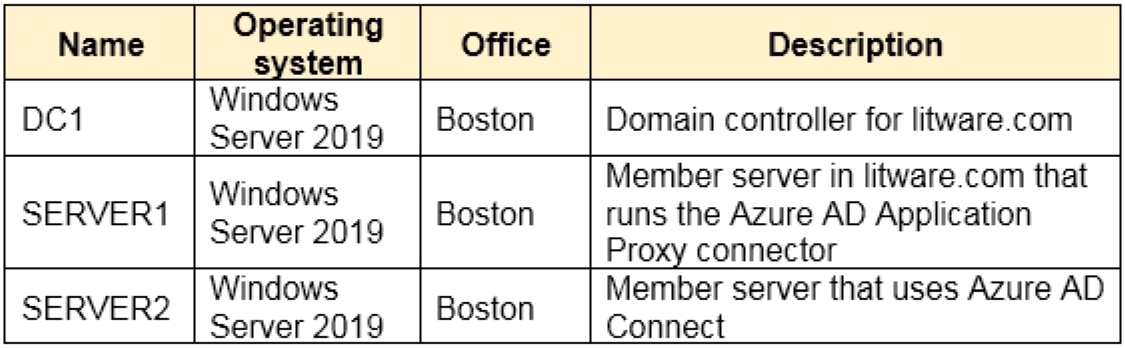
Answer Area

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

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.

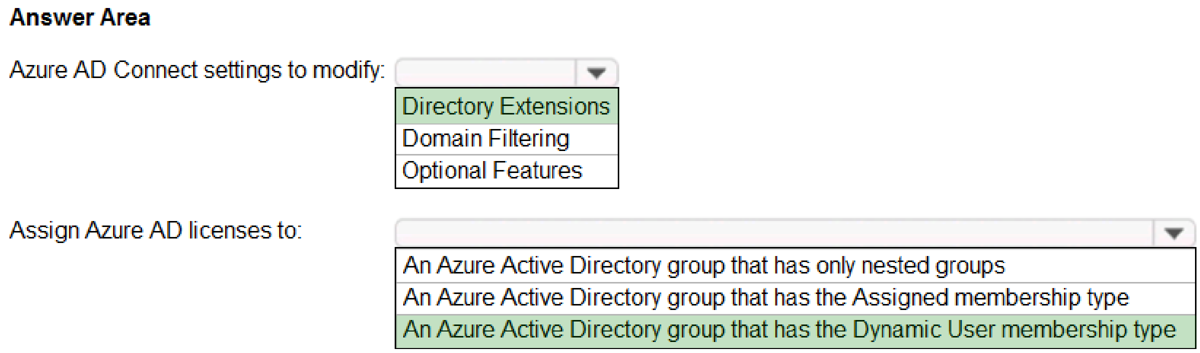
Control privileged access to applications by using access reviews in Azure AD.

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 #75

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]

Question #76

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.

Question #77

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

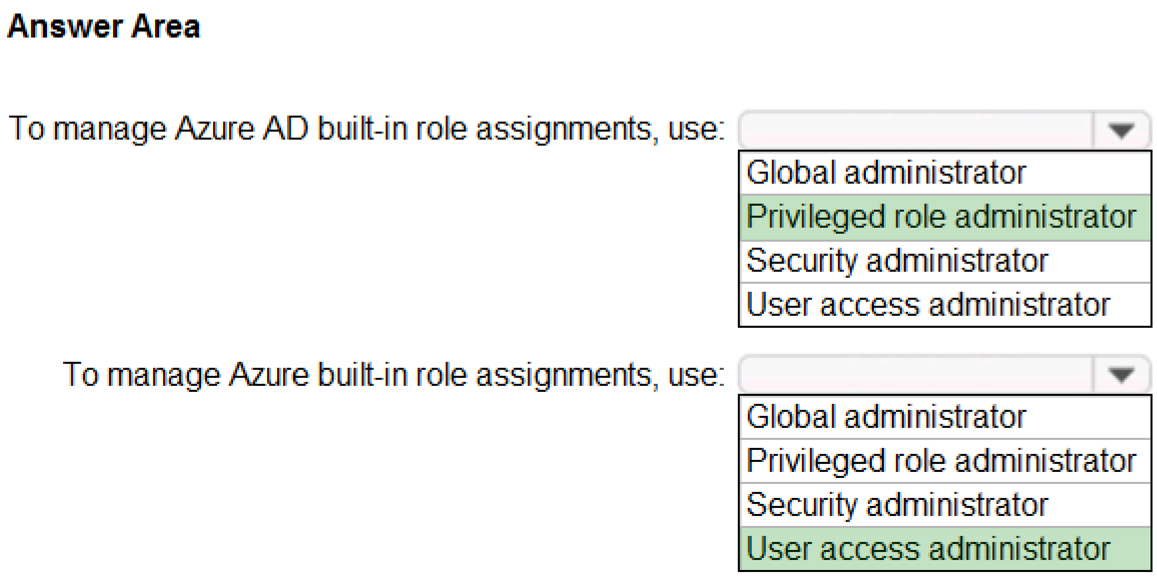
Question #78

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]

Question #79

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:

```
(user.objectid -ne "null") and (user.usertype -eq "member")
```

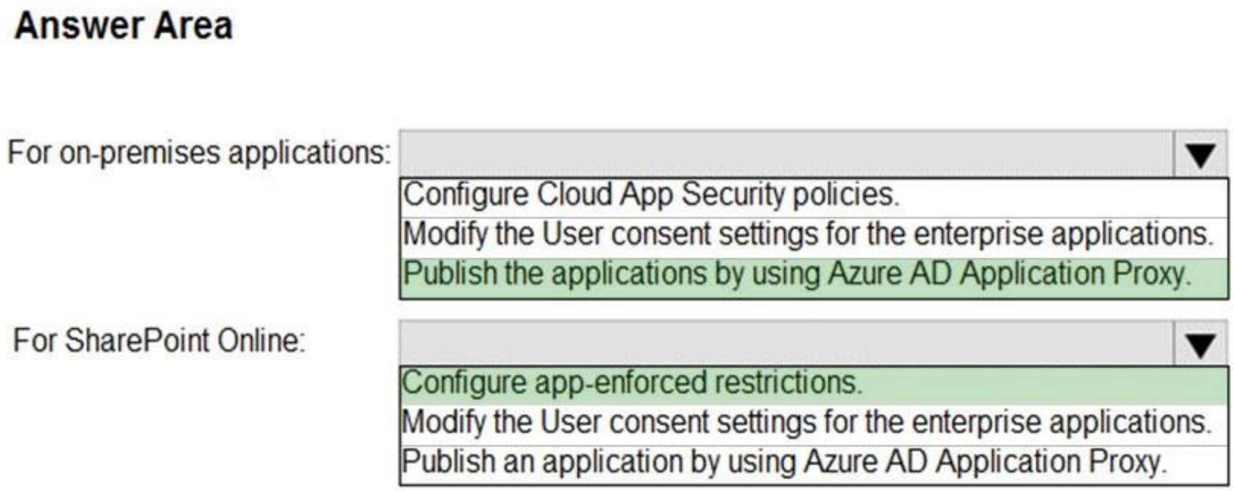
Question #80

You need to implement on-premises application and SharePoint Online restrictions to meet the authentication requirements and the access requirements.

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

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

For on-premises applications:

- Configure Cloud App Security policies.
- Modify the User consent settings for the enterprise applications.
- [✓ Publish the applications by using Azure AD Application Proxy.]

For SharePoint Online:

- [✓ Configure app-enforced restrictions.]
- Modify the User consent settings for the enterprise applications.
- Publish an application by using Azure AD Application Proxy.

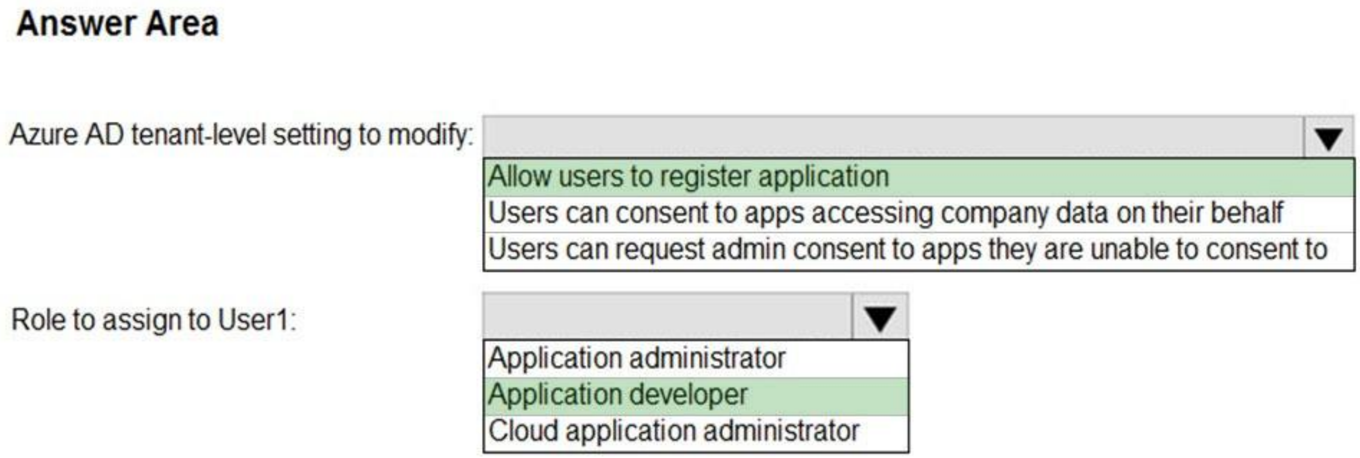
Question #81

You need to configure app registration in Azure AD to meet the delegation requirements.

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

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

Azure AD tenant-level setting to modify:

- [✓ Allow users to register application]
- Users can consent to apps accessing company data on their behalf
- Users can request admin consent to apps they are unable to consent to

Role to assign to User1:

- Application administrator
- [✓ Application developer]
- Cloud application administrator

Question #82

You need to configure the detection of multi-staged attacks to meet the monitoring requirements.
What should you do?

- A. Customize the Azure Sentinel rule logic.
- B. Create a workbook.
- **C**. Add Azure Sentinel data connectors.
- D. Add an Azure Sentinel playbook.

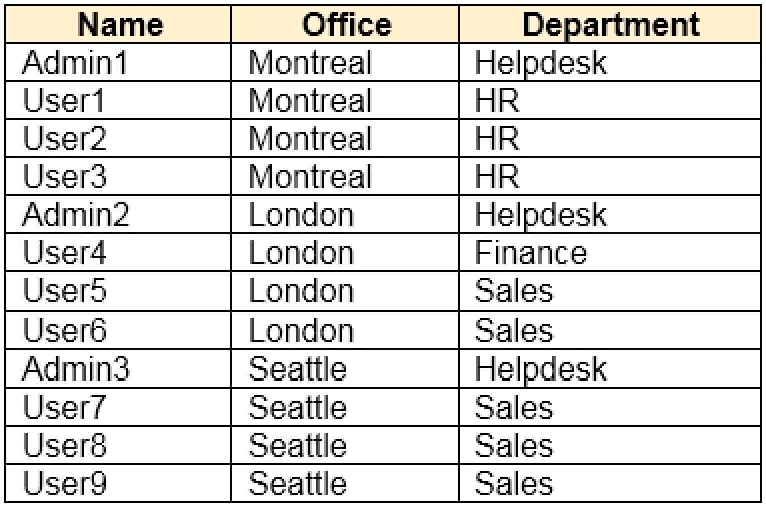
Question #83

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.

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 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.

Requirement. 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.

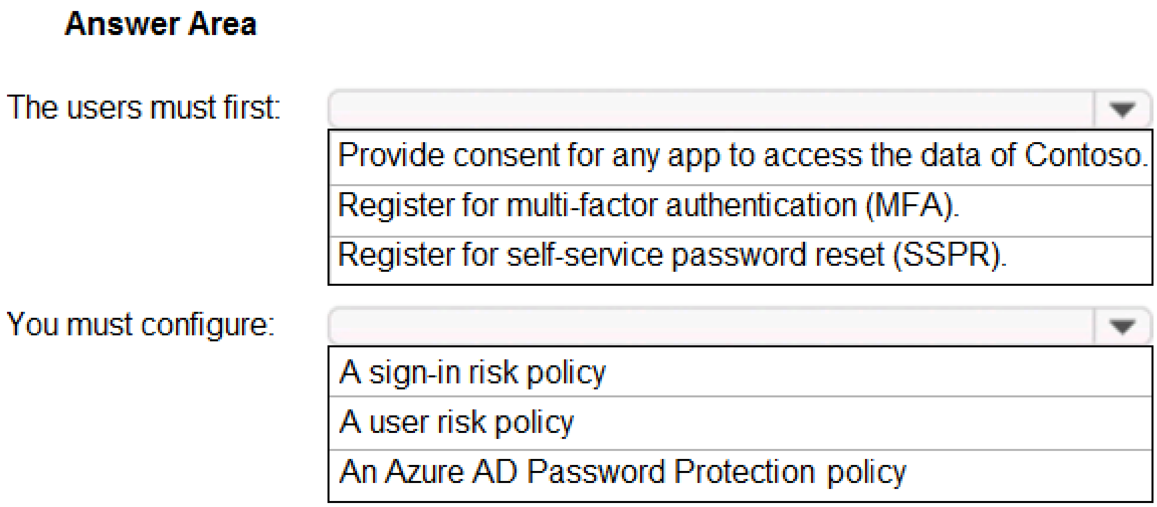
Fabrikam users must have access to the marketing departmentג€™s SharePoint site for a maximum of 90 days.

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 usersג€™ identity was compromised.

Question #84
You need to meet the technical requirements for the probability that user identities were compromised.
What should the users do first, and what should you configure? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:



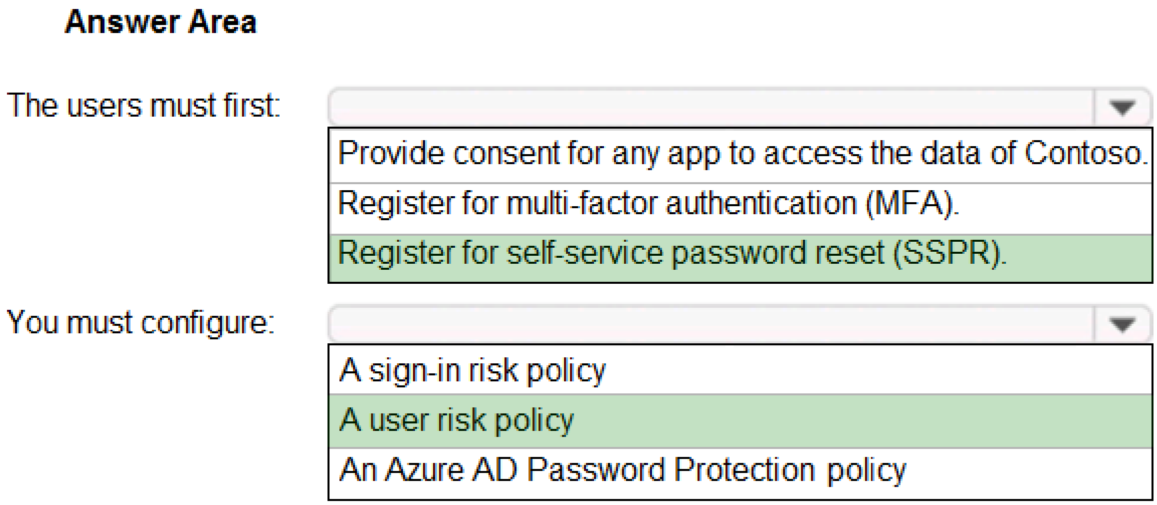
Answer Area

The users must first:

- Provide consent for any app to access the data of Contoso.
- Register for multi-factor authentication (MFA).
- Register for self-service password reset (SSPR).

You must configure:

- A sign-in risk policy
- A user risk policy
- An Azure AD Password Protection policy



Answer 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

Question #85

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

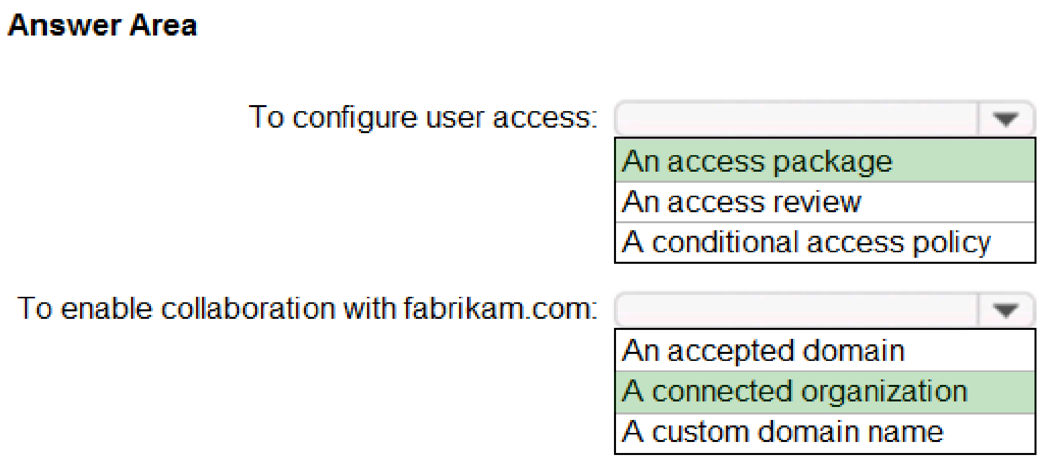
Question #86

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

Question #87

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.



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

Question #88

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.