Microsoft.SC-300.vJan-2024.byLioanRun.100q

Number: SC-300
Passing Score: 800
Time Limit: 120
File Version: 17.0

Exam Code: SC-300
Exam Name: Microsoft Identity and Access Administrator

Case Study 01

Litware, Inc

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.

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.

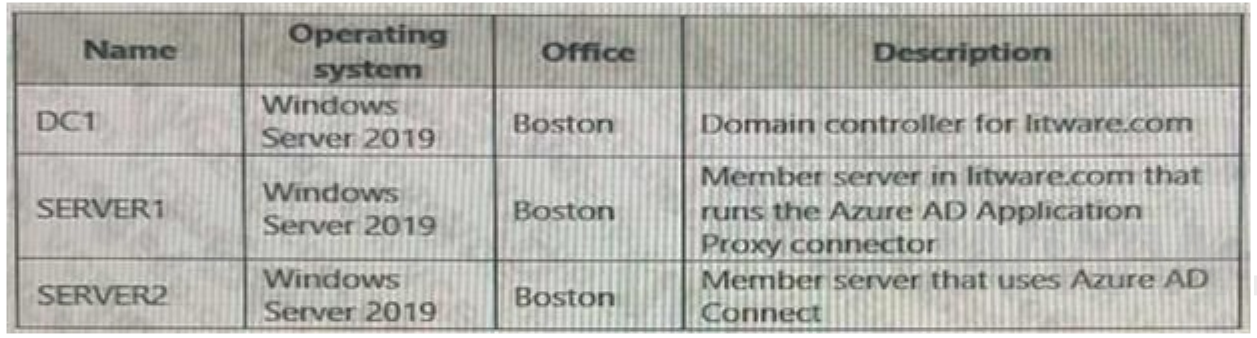
Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection polices 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.

On-premises Environment

The on-premises network contains the severs 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.

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 catalogs and custom programs for Identity Governance.

* Ensure that User1 can create enterprise applications in Azure AD. Use the principle of least privilege.

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 Microsoft 365 group that he appropriate license assigned.

Management Requirement

Litware wants to create a group named LWGroup1 will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.

Authentication Requirements

Litware identifies the following authentication requirements:

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

Access 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.

Monitoring Requirements

Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity.

QUESTION 1

HOTSPOT

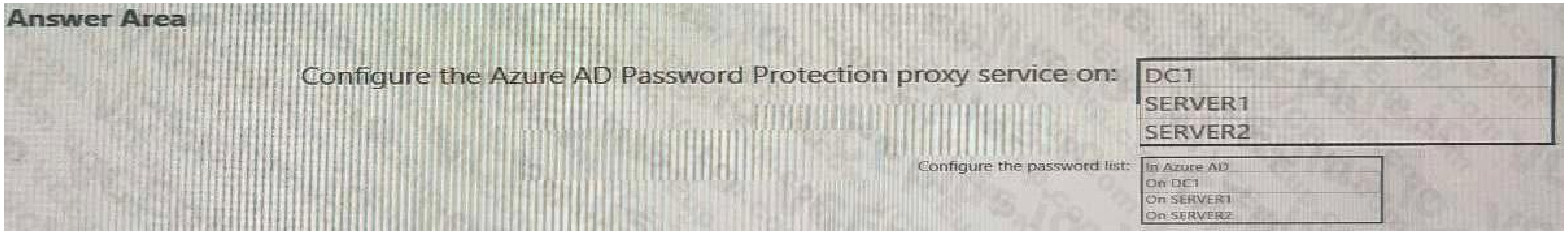
You need to implement password restrictions to meet the authentication requirements.

You install the Azure AD password Protection DC agent on DC1.

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

NOTE: Each correct selection is worth one point.

Hot Area:

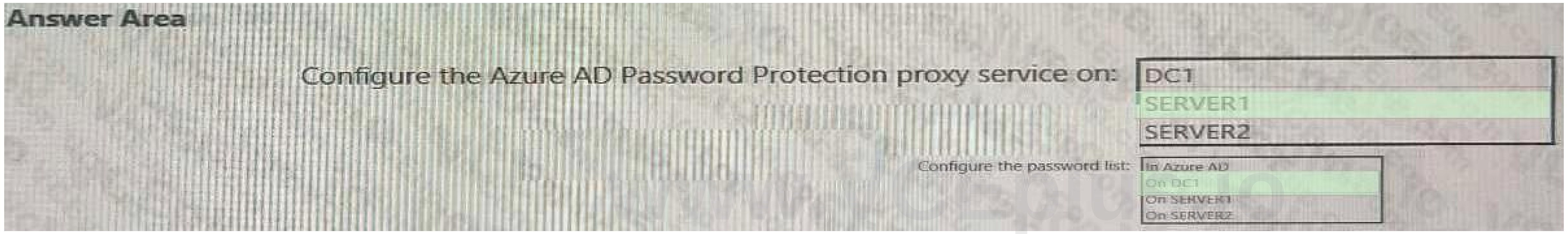


Answer Area

Configure the Azure AD Password Protection proxy service on:
- DC1
- SERVER1
- SERVER2

Configure the password list:
- In Azure AD
- On DC1
- On SERVER1
- On SERVER2

Answer Area:



Answer Area

Configure the Azure AD Password Protection proxy service on:
- DC1
- [✓ SERVER1]
- SERVER2

Configure the password list:
- In Azure AD
- [✓ On DC1]
- On SERVER1
- On SERVER2

Section:

Explanation:

QUESTION 2

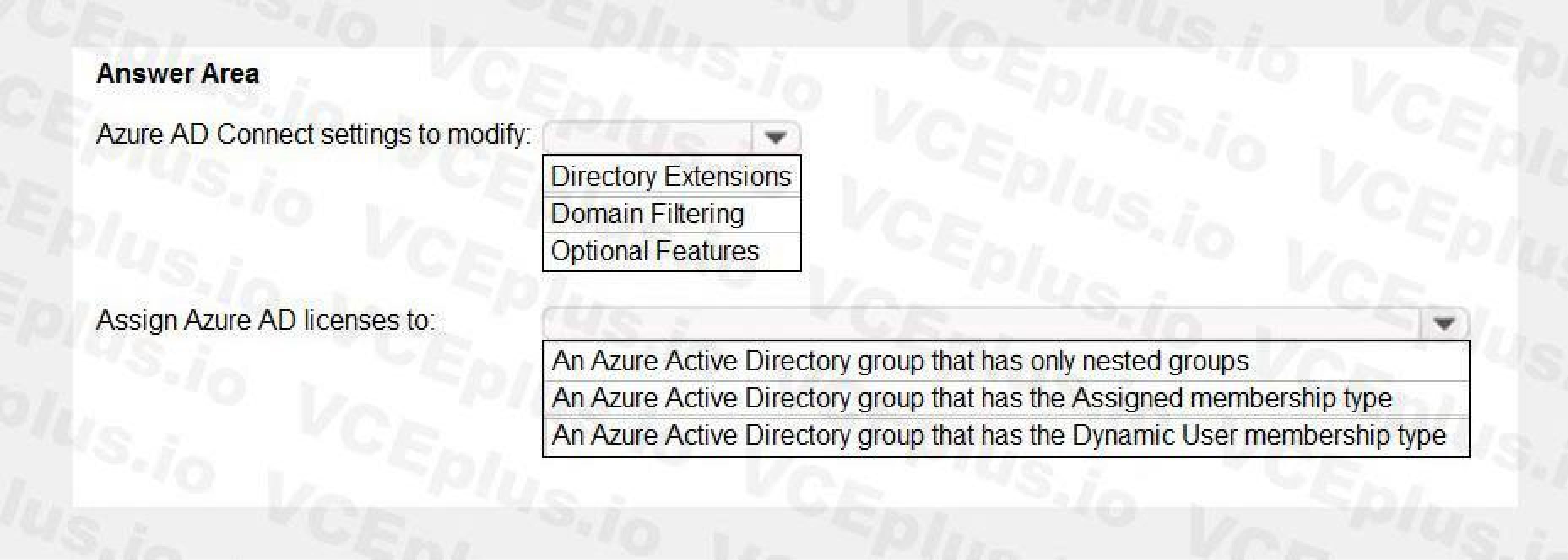
HOTSPOT

You need to configure the assignment of Azure AD licenses to the Litware users. The solution must meet the licensing requirements.

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

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

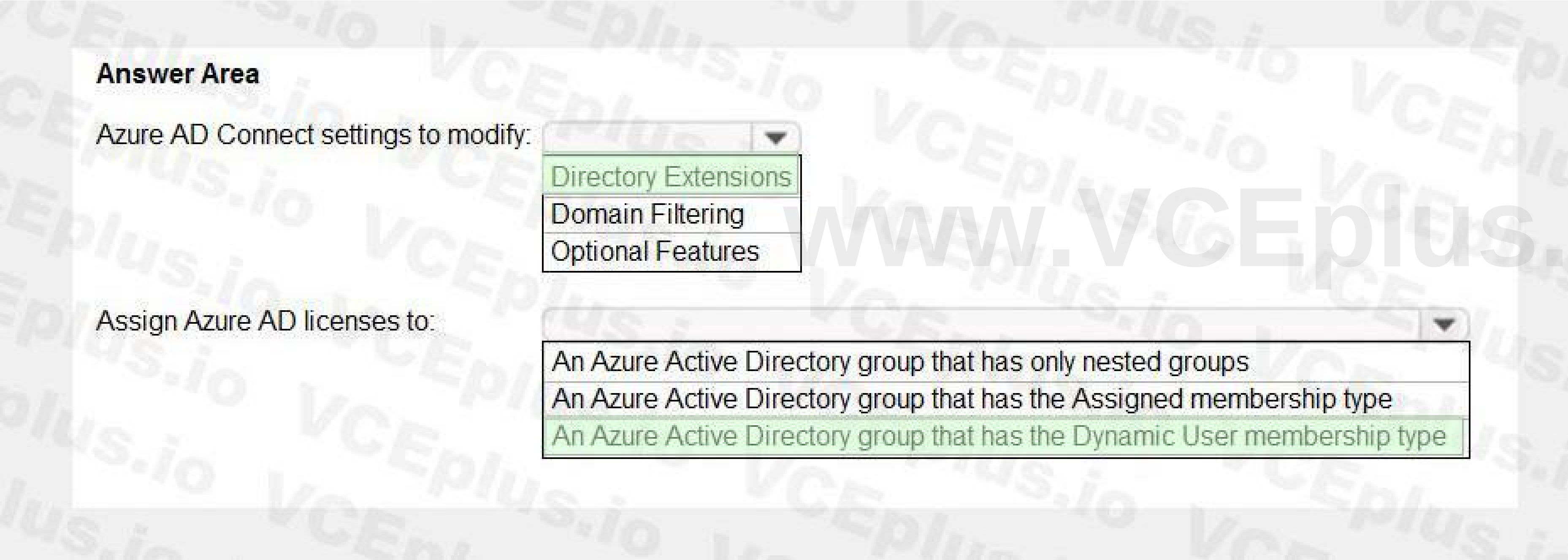
Azure AD Connect settings to modify:

- Directory Extensions
- Domain Filtering
- Optional Features

Assign Azure AD licenses to:

- An Azure Active Directory group that has only nested groups
- An Azure Active Directory group that has the Assigned membership type
- An Azure Active Directory group that has the Dynamic User membership type

Answer 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]

Section:

Explanation:

Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest. Litware wants to manage the assignment of Azure AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to a Microsoft 365 group that has the appropriate licenses assigned.

QUESTION 3

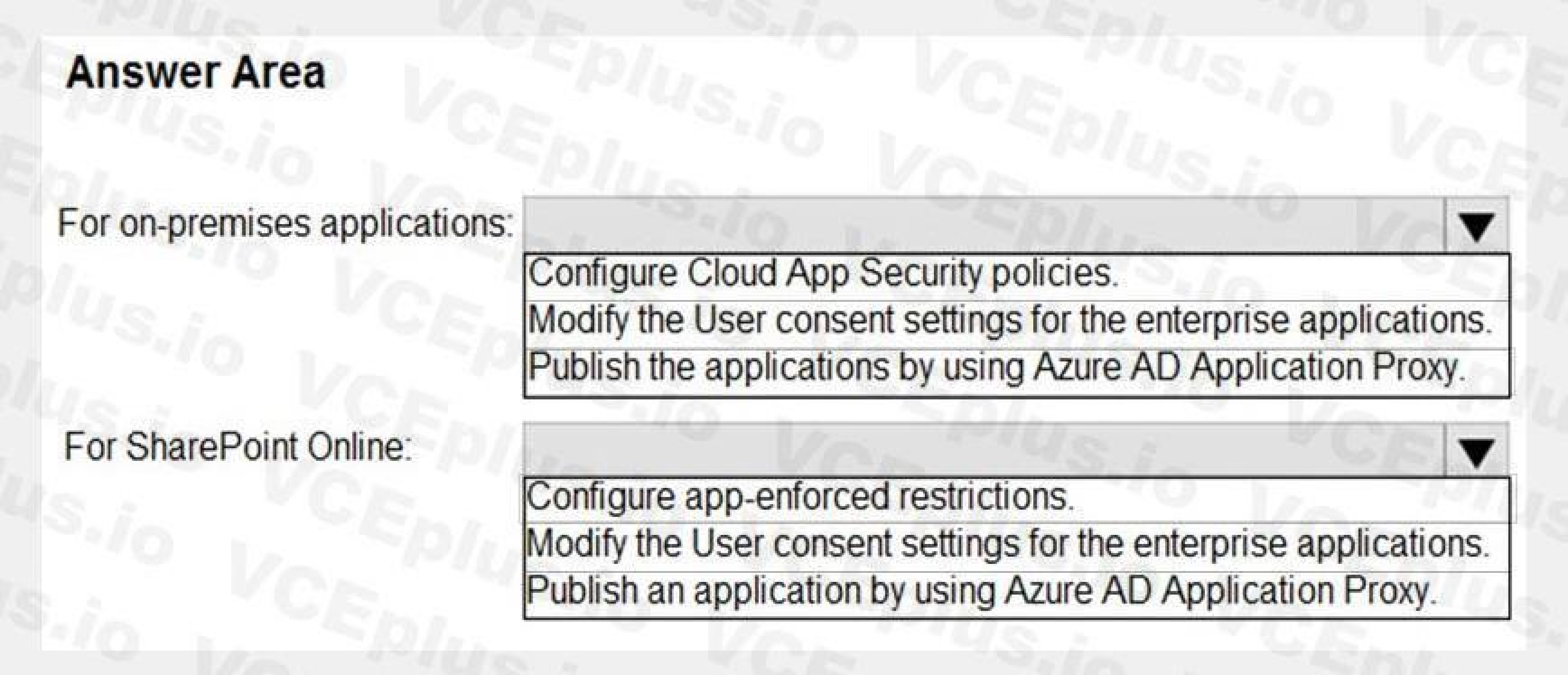
HOTSPOT

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

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

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

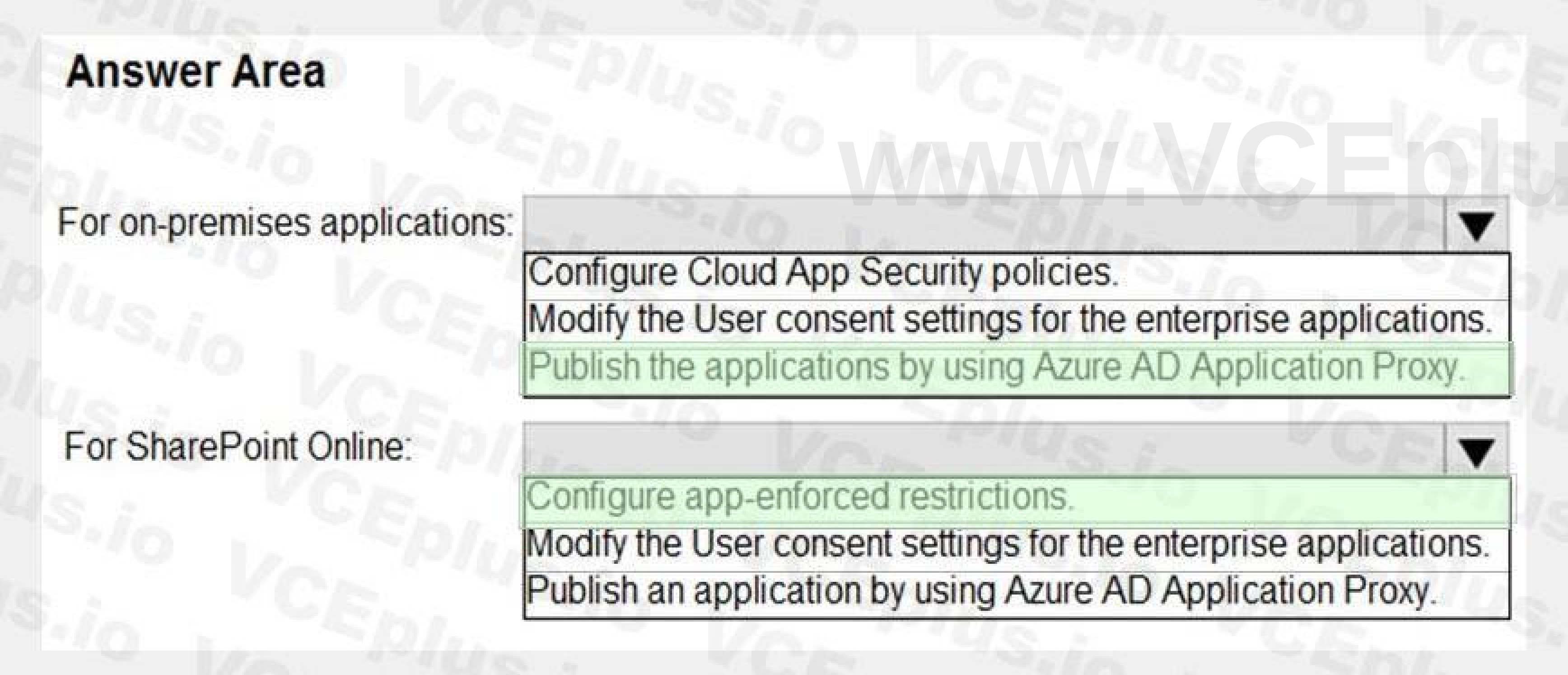
For on-premises applications:

- 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.

Answer 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:

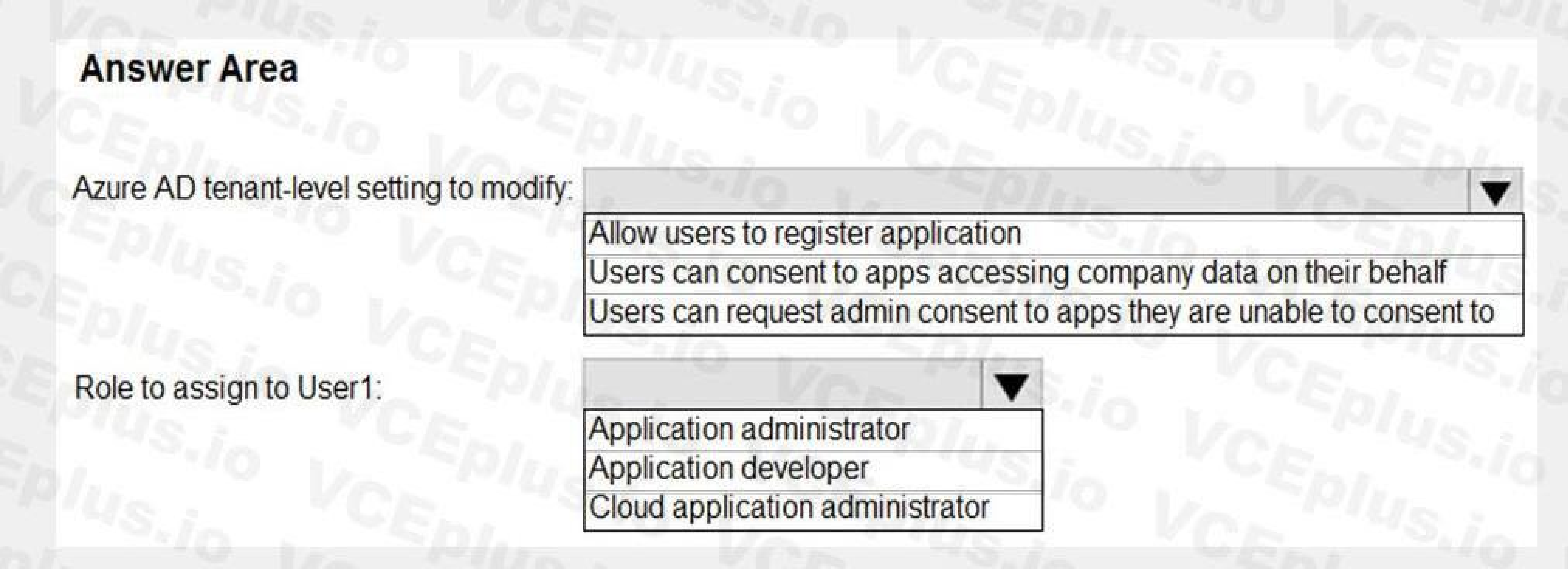
- [✓ Configure app-enforced restrictions.]
- Modify the User consent settings for the enterprise applications.
- Publish an application by using Azure AD Application Proxy.

Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/sharepoint/app-enforced-restrictions
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session

QUESTION 4
HOTSPOT
You need to configure app registration in Azure AD to meet the delegation requirements.
What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

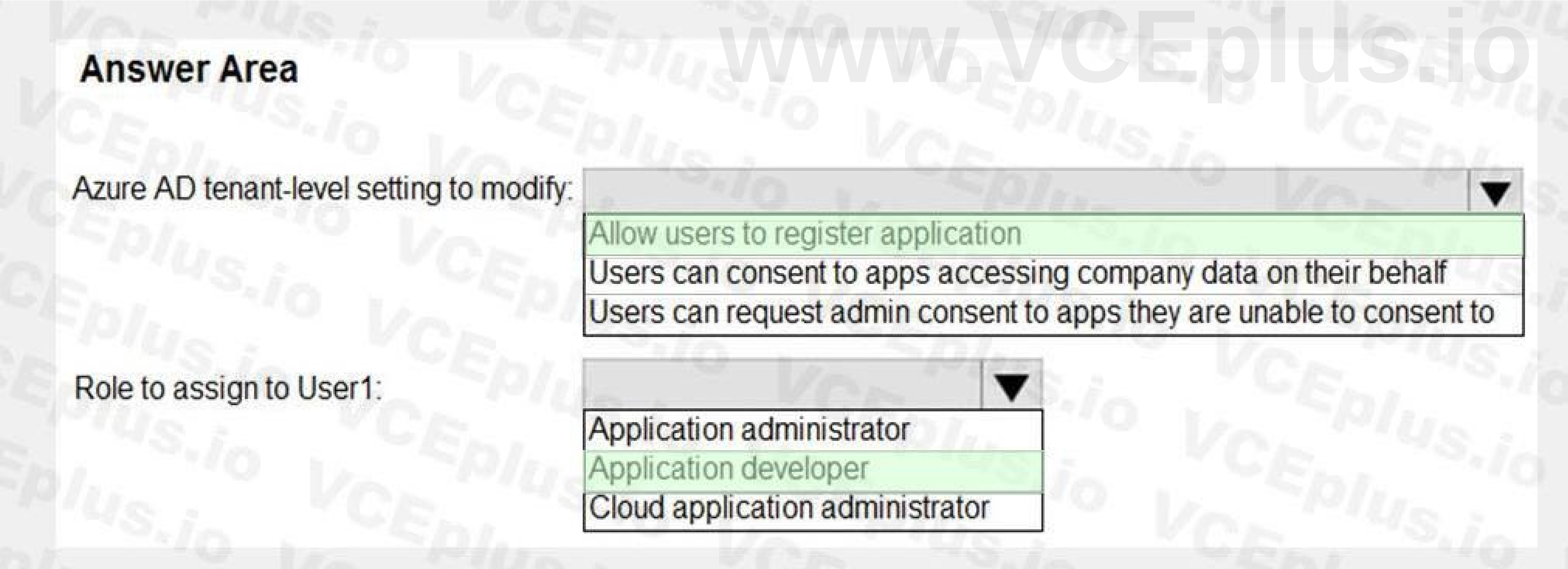
Azure AD tenant-level setting to modify:

- 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

Answer 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:

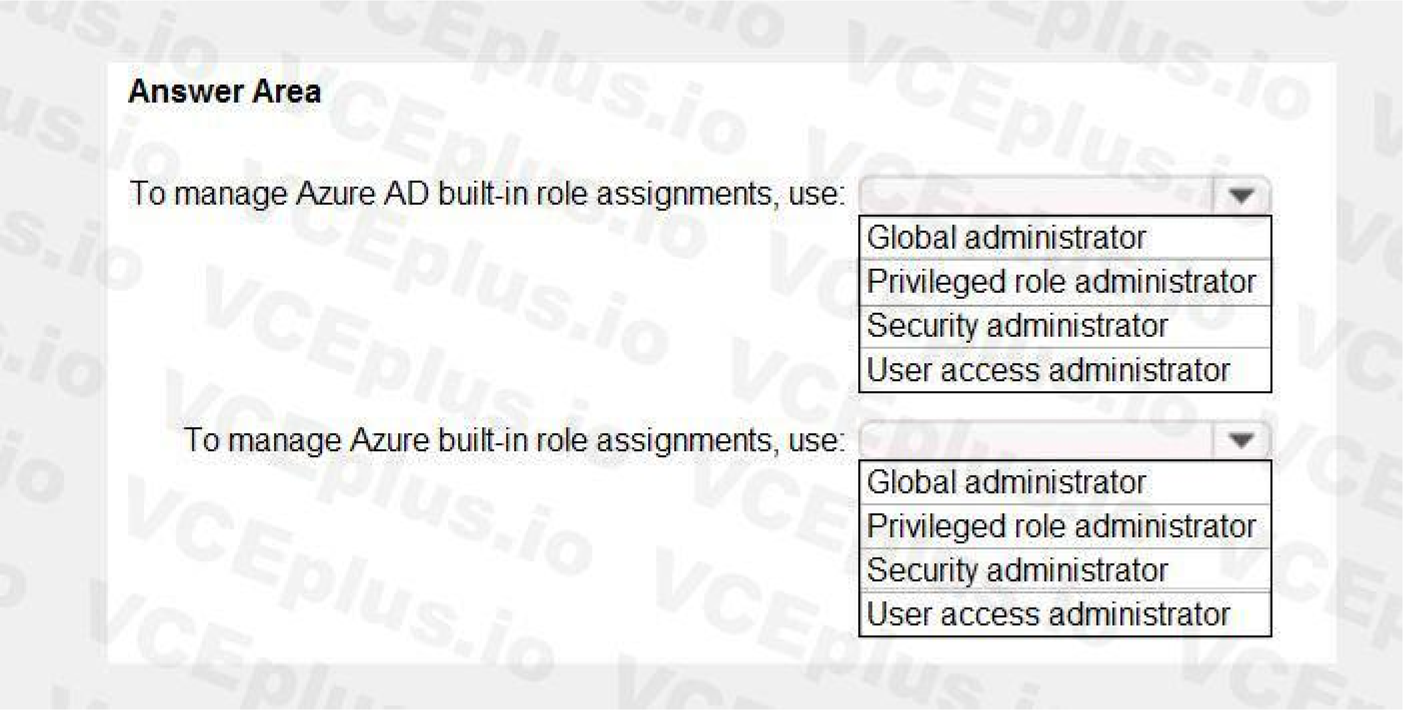
- Application administrator
- [✓ Application developer]
- Cloud application administrator

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

QUESTION 5
HOTSPOT

You need to identify which roles to use for managing role assignments. The solution must meet the delegation requirements.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

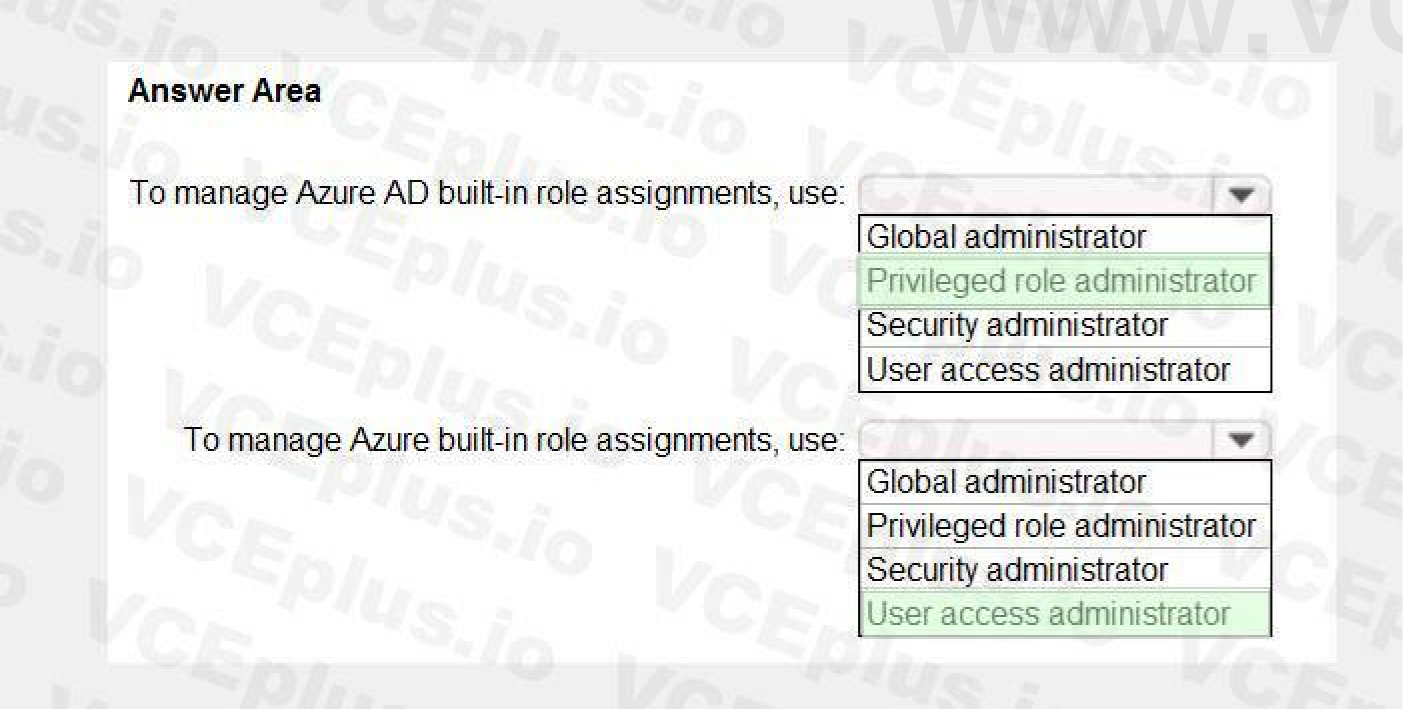
To manage Azure AD built-in role assignments, use:

- Global administrator
- Privileged role administrator
- Security administrator
- User access administrator

To manage Azure built-in role assignments, use:

- Global administrator
- Privileged role administrator
- Security administrator
- User access administrator

Answer 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]

Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

QUESTION 6

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 configure?

A. named locations that have a private IP address range
B. named locations that have a public IP address range
C. trusted IPs that have a public IP address range
D. trusted IPs that have a private IP address range

Correct Answer: C
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-conditionLocation offer your country set, IP ranges MFA trusted IP and corporate network VPN gateway IP address: This is the public IP address of the VPN device for your on-premises network. The VPN device requires an IPv4 public IP address. Specify a valid public IP address for the VPN device to which you want to connect. It must be reachable by Azure Client Address space: List the IP address ranges that you want routed to the local on-premises network through this gateway. You can add multiple address space ranges. Make sure that the ranges you specify here do not overlap with ranges of other networks your virtual network connects to, or with the address ranges of the virtual network itself.

QUESTION 7
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 an Azure Sentinel playbook.
D. Add Azure Sentinel data connectors.

Correct Answer: D
Section:

QUESTION 8
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.

Correct Answer: A
Section:

QUESTION 9
You need to track application access assignments by using Identity Governance. The solution must meet the delegation requirements.
What should you do first?

A. Modify the User consent settings for the enterprise applications.
B. Create a catalog.

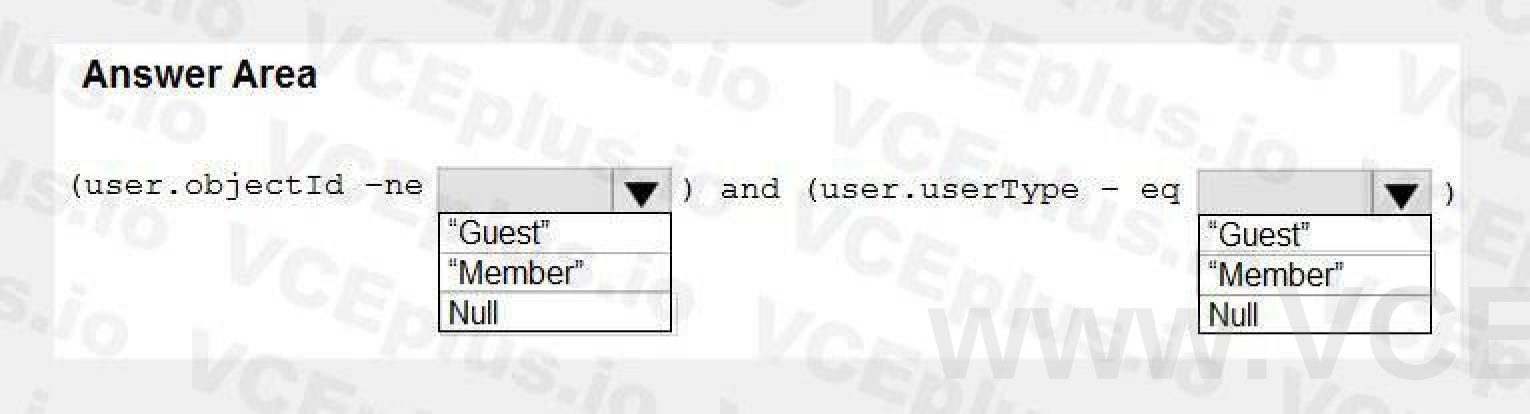
C. Create a program.

D. Modify the Admin consent requests settings for the enterprise applications.

Correct Answer: B
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-managementoverview

QUESTION 10
HOTSPOT
You need to create the LWGroup1 group to meet the management requirements.
How should you complete the dynamic membership rule? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



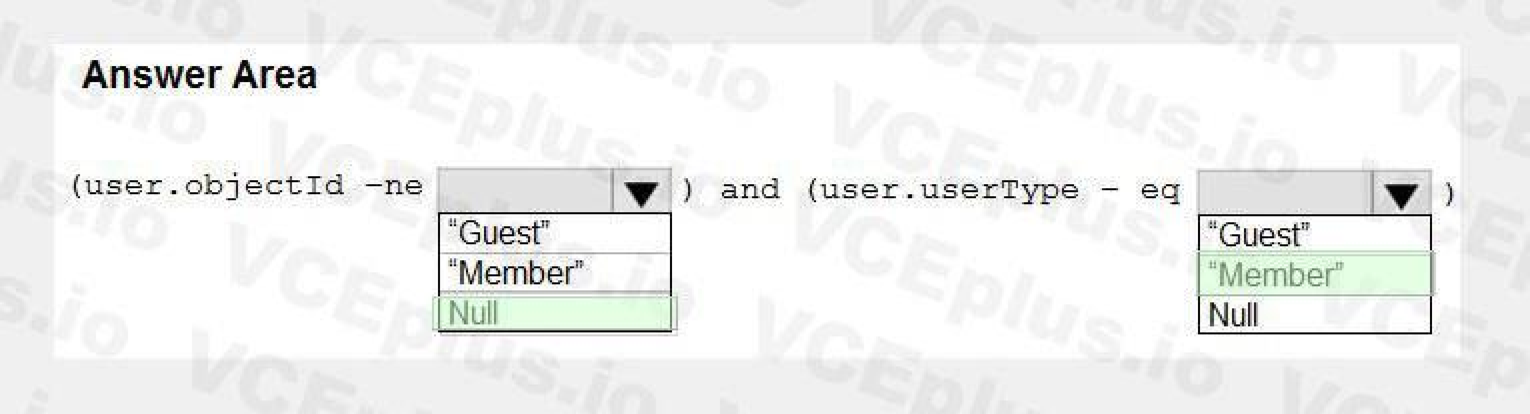
Answer Area

(user.objectId -ne ▼) and (user.userType – eq ▼)

"Guest"
"Member"
Null

"Guest"
"Member"
Null

Answer Area:



Answer Area

(user.objectId -ne ▼) and (user.userType – eq ▼)

"Guest"
"Member"
[✓ Null]

"Guest"
[✓ "Member"]
Null

Section:
Explanation:

Case Study 03
A Datum Corp
Overview
A Datum Corporation is a consulting company in Montreal.
A Datum recently acquired a Vancouver-based company named Litware, Inc.
A Datum Environment
The on-premises network of A. Datum contains an Active Directory Domain Services (AD DS) forest named adatum.com.
A Datum has a Microsoft 365 E5 subscription. The subscription contains a verified domain that syncs with the adatum.com AD DS domain by using Azure AD Connect.
A Datum has an Azure Active Directory (Azure AD) tenant named adatum.com. The tenant has Security defaults disabled.

The tenant contains the users shown in the following table.

Problem Statements

A Datum identifies the following issues:

•bullet Multiple users in the sales department have up to five devices. The sales department users report that sometimes they must contact the support department to join their devices to the Azure AD tenant because they have reached their device limit.

•bullet A recent security incident reveals that several users leaked their credentials, a suspicious browser was used for a sign-in, and resources were accessed from an anonymous IP address,

•bullet When you attempt to assign the Device Administrators role To IT_Group1, the group does NOT appear in the selection list.

•bullet Anyone in the organization can invite guest users, including other guests and non-administrators.

•bullet The helpdesk spends too much time resetting user passwords.

•bullet Users currently use only passwords for authentication.

Requirements

A, Datum plans to implement the following changes;

•bullet Configure self-service password reset {SSPR}.

•bullet Configure multi-factor authentication (MFA) for all users.

•bullet Configure an access review for an access package named Package1.

•bullet Require admin approval for application access to organizational data.

•bullet Sync the AD DS users and groupsoflitware.com with the Azure AD tenant.

•bullet Ensure that only users that are assigned specific admin roles can invite guest users.

•bullet Increase the maximum number of devices that can be joined or registered to Azure AD to 10.

Technical Requirements

A. Datum identifies the following technical requirements:

•bullet Users assigned the User administrator role must be able to request permission to use the role when needed for up to one year.

•bullet Users must be prompted to register for MFA and provided with an option to bypass the registration for a grace period.

•bullet Users must provide one authentication method to reset their password by using SSPR. Available methods must include:

•bullet Email

•bullet Phone

•bullet Security questions

•bullet The Microsoft Authenticator app

•bullet Trust relationships must NOT be established between the adatum.com and litware.com AD DS domains.

•bullet The principle of least privilege must be used.

QUESTION 1

You need to implement the planned changes for litware.com. What should you configure?

A. Azure AD Connect cloud sync between the Azure AD tenant and litware.com

B. Azure AD Connect to include the litware.com domain

C. staging mode in Azure AD Connect for the litware.com domain

Correct Answer: C

Section:

QUESTION 2

You need implement the planned changes for application access to organizational data. What should you configure?

A. authentication methods

B. the User consent settings

C. access packages

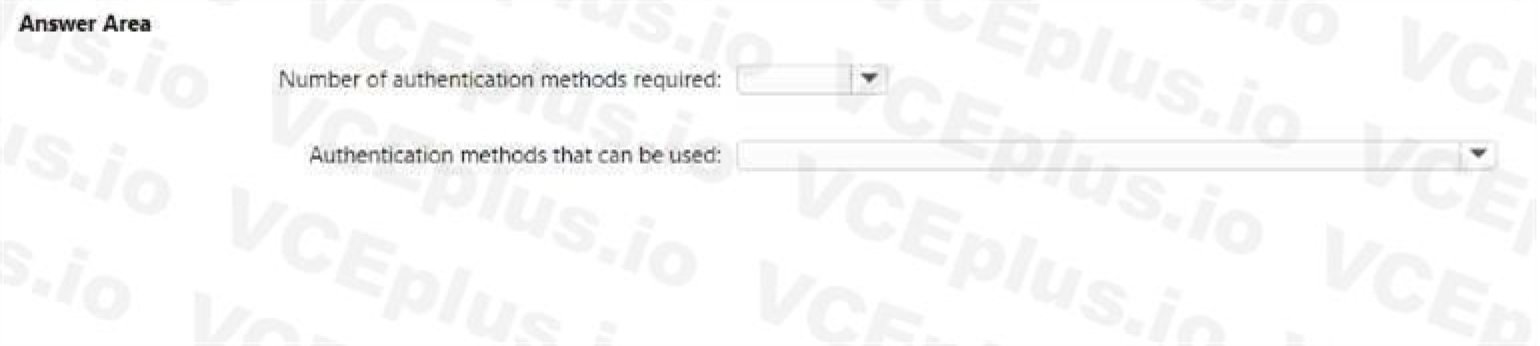
D. an application proxy

Correct Answer: B

Section:

QUESTION 3

You implement the planned changes for SSPR.
What occurs when User3 attempts to use SSPR? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

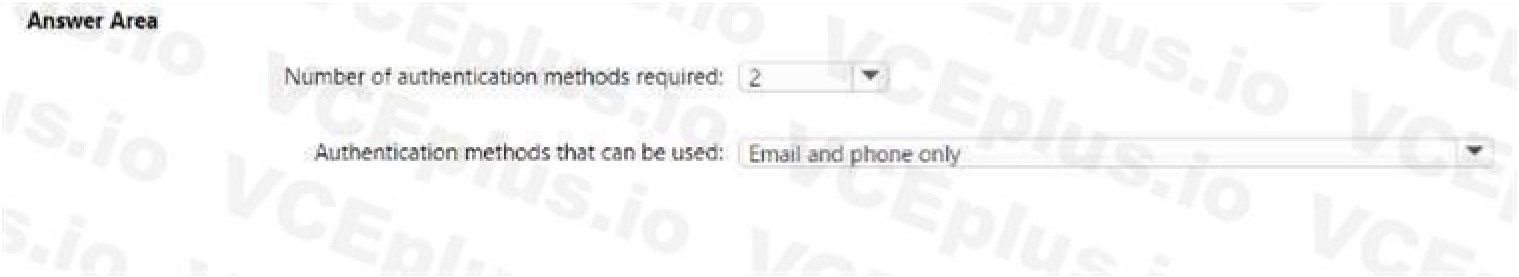


Answer Area

Number of authentication methods required:

Authentication methods that can be used:

A.



Answer Area

Number of authentication methods required: 2

Authentication methods that can be used: Email and phone only

Correct Answer: A
Section:

QUESTION 4

You need to resolve the issue of the sales department users. What should you configure for the Azure AD tenant?

A. the User settings
B. the Device settings
C. the Access reviews settings
D. Security defaults

Correct Answer: B
Section:

QUESTION 5
You need to resolve the issue of I-.Group1. What should you do first?

A. Recreate the IT-Group 1 group.
B. Change Membership type of IT-Group1 to Dynamic Device
C. Add an owner to IT_Group1.
D. Change Membership type of IT-Group1 to Dynamic User

Correct Answer: A
Section:

QUESTION 6

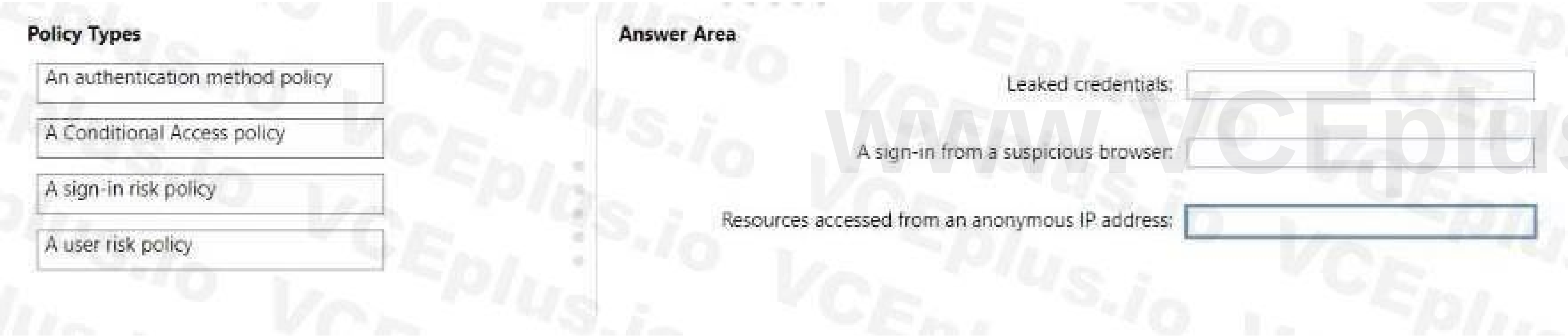
You need to implement the planned changes for Package1. Which users can create and manage the access review?

A. User3 only
B. User4 only
C. User5 only
D. User3 and User4
E. User3 and User5
F. User4and User5

Correct Answer: E
Section:

QUESTION 7
DRAG DROP
You need to resolve the recent security incident issues.
What should you configure for each incident? To answer, drag the appropriate policy types to the correct issues. Each policy type may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.

Select and Place:



Policy Types

- An authentication method policy
- A Conditional Access policy
- A sign-in risk policy
- A user risk policy

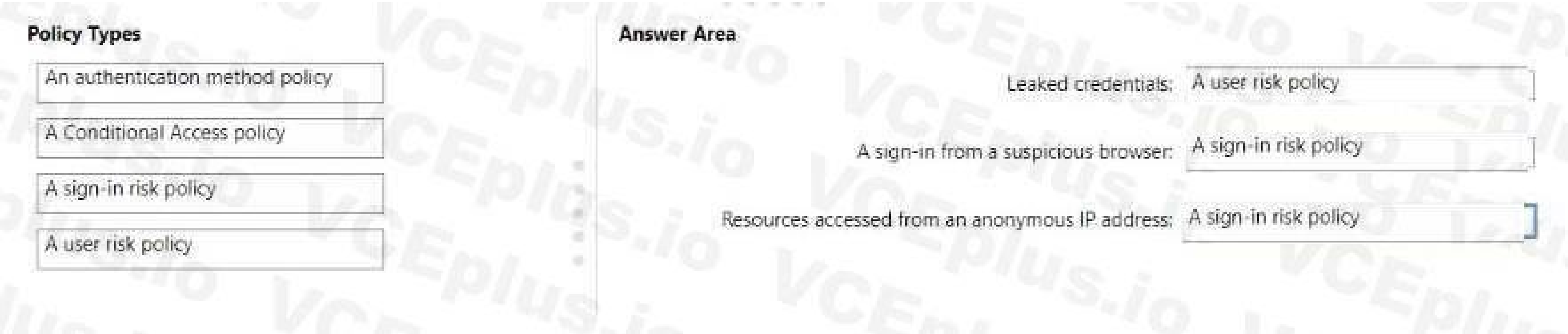
Answer Area

Leaked credentials:

A sign-in from a suspicious browser:

Resources accessed from an anonymous IP address:

Correct Answer:



Policy Types

- An authentication method policy
- A Conditional Access policy
- A sign-in risk policy
- A user risk policy

Answer Area

Leaked credentials: A user risk policy

A sign-in from a suspicious browser: A sign-in risk policy

Resources accessed from an anonymous IP address: A sign-in risk policy

Section:
Explanation:

QUESTION 8
You need to resolve the issue of the guest user invitations. What should you do for the Azure AD tenant?

A. Configure the Continuous access evaluation settings.

B. Modify the External collaboration settings.

C. Configure the Access reviews settings.

D. Configure a Conditional Access policy.

Correct Answer: B
Section:

QUESTION 9
You need to modify the settings of the User administrator role to meet the technical requirements. Which two actions should you perform for the role? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Select Require justification on activation

B. Set all assignments to Active

C. Set all assignments to Eligible

D. Modify the Expire eligible assignments after setting.

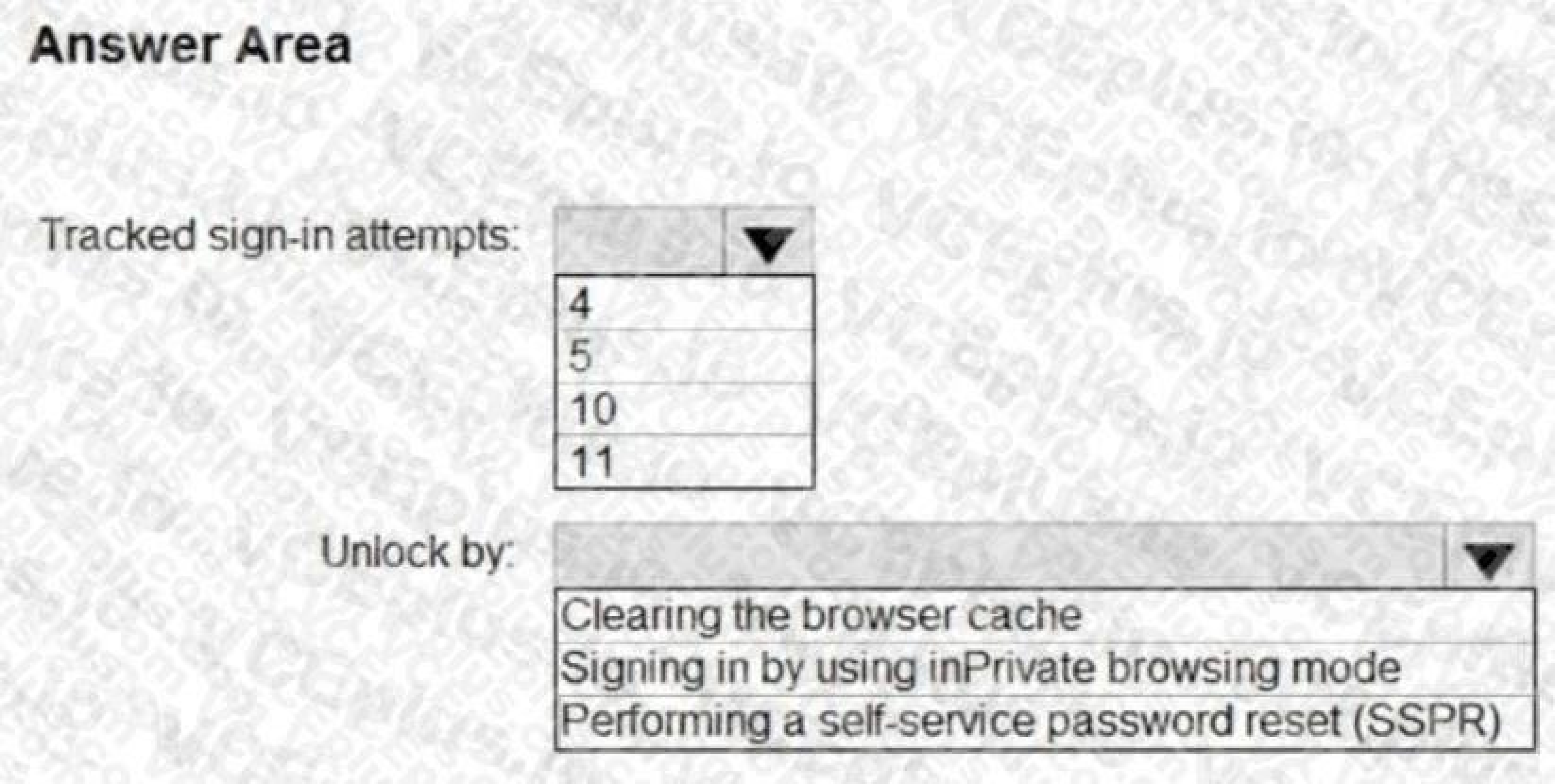
E. Select Require ticket information on activation.

Correct Answer: A, B
Section:

Exam A

QUESTION 1
HOTSPOT
A user named User1 attempts to sign in to the tenant by entering the following incorrect passwords:
Pa55w0rd12
Pa55w0rd12
Pa55w0rd12
Pa55w.rd12
Pa55w.rd123
Pa55w.rd123
Pa55w.rd123
Pa55word12
Pa55word12
Pa55word12
Pa55w.rd12 You need to identify how many sign-in attempts were tracked for User1, and how User1 can unlock her account before the 300-second lockout duration expires. What should identify? To answer, select the appropriate
NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

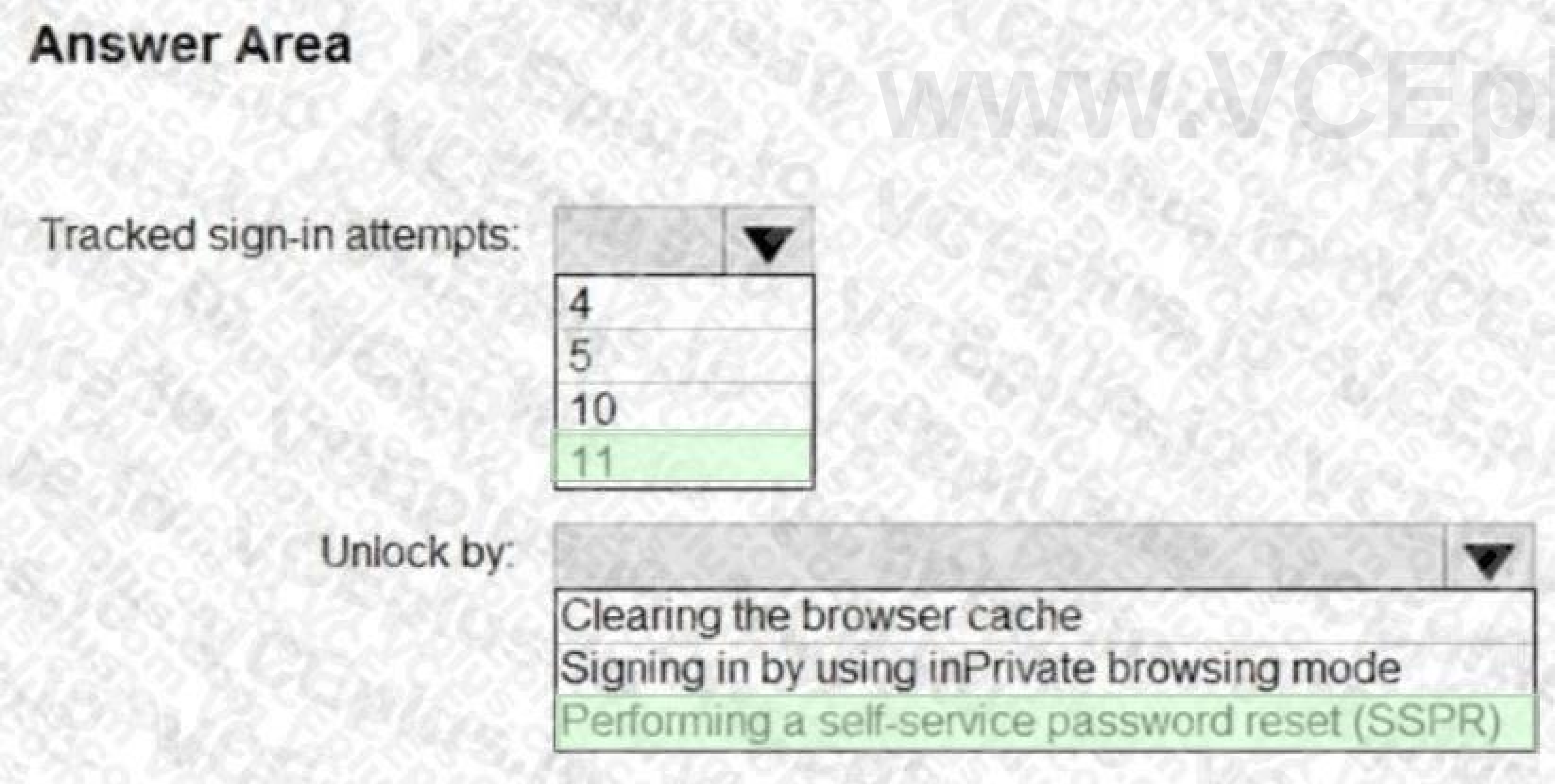
Tracked sign-in attempts:

4
5
10
11

Unlock by:

Clearing the browser cache
Signing in by using inPrivate browsing mode
Performing a self-service password reset (SSPR)

Answer Area:



Answer Area

Tracked sign-in attempts:

4
5
10
[✓ 11]

Unlock by:

Clearing the browser cache
Signing in by using inPrivate browsing mode
[✓ Performing a self-service password reset (SSPR)]

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

QUESTION 2

HOTSPOT

You have an Azure subscription.

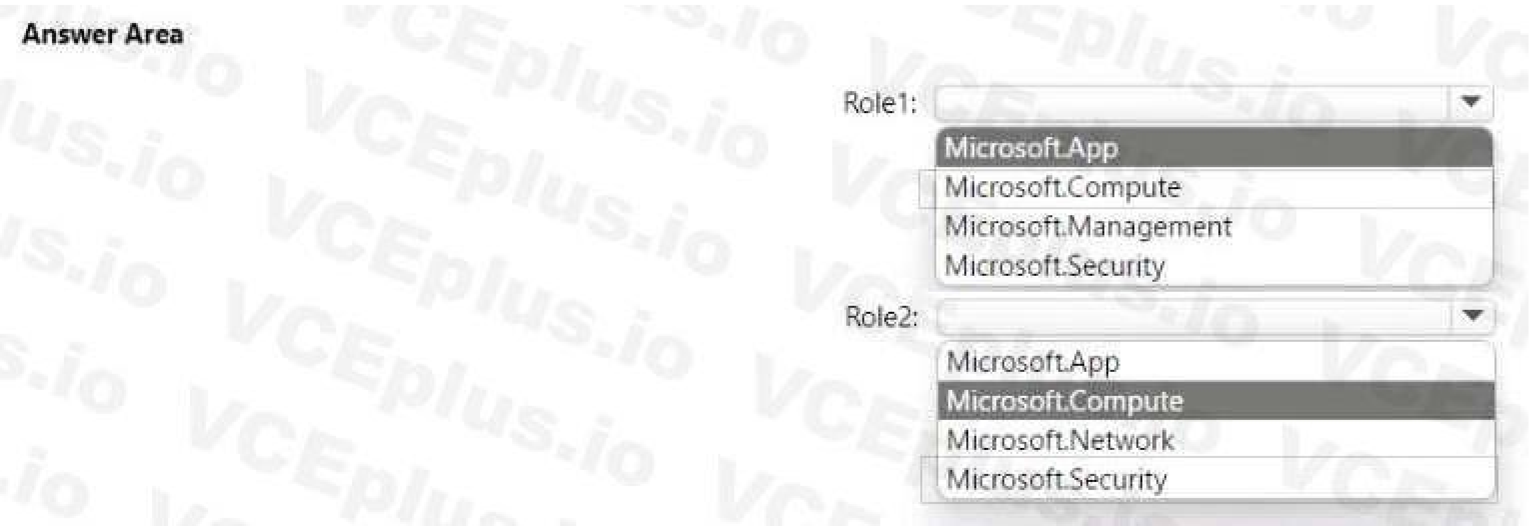
You need to create two custom roles named Role1 and Role2. The solution must meet the following requirements:

- Users that are assigned Role1 can create or delete instances of Azure Container Apps.
- Users that are assigned Role2 can enforce adaptive network hardening rules.

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

NOTE: Each correct selection is worth one point.

Hot Area:

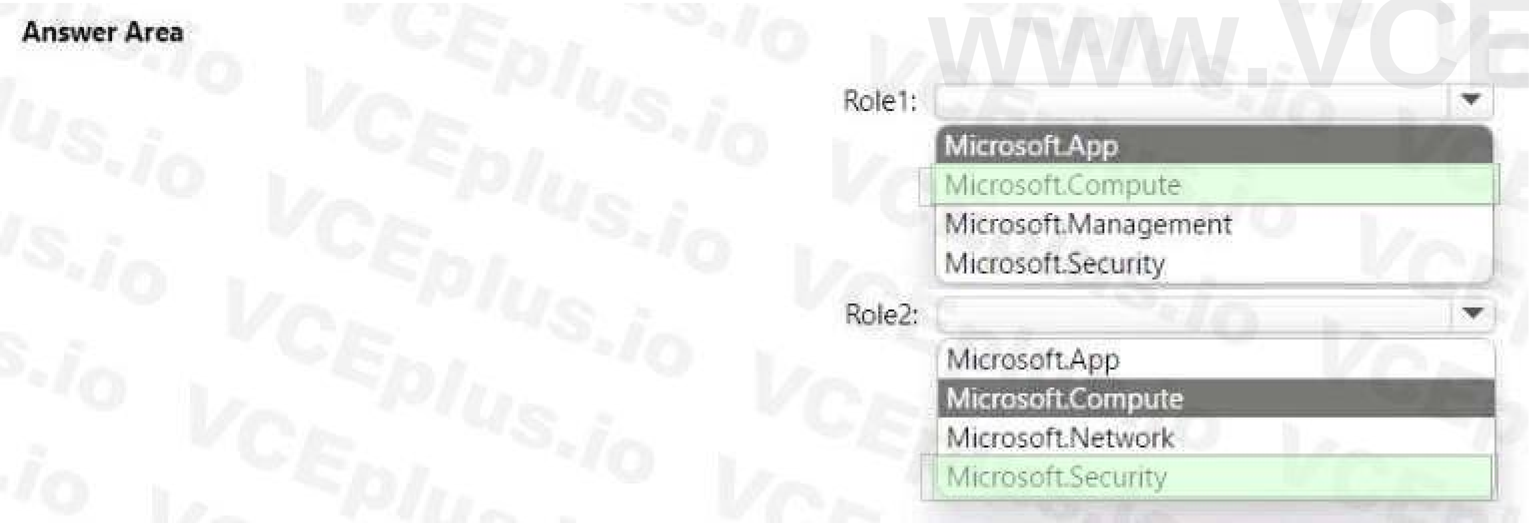


Answer Area

Role1:
- Microsoft.App
- Microsoft.Compute
- Microsoft.Management
- Microsoft.Security

Role2:
- Microsoft.App
- Microsoft.Compute
- Microsoft.Network
- Microsoft.Security

Answer Area:



Answer Area

Role1:
- Microsoft.App
- Microsoft.Compute
- Microsoft.Management
- Microsoft.Security

Role2:
- Microsoft.App
- Microsoft.Compute
- Microsoft.Network
- Microsoft.Security

Section:

Explanation:

QUESTION 3

DRAG DROP

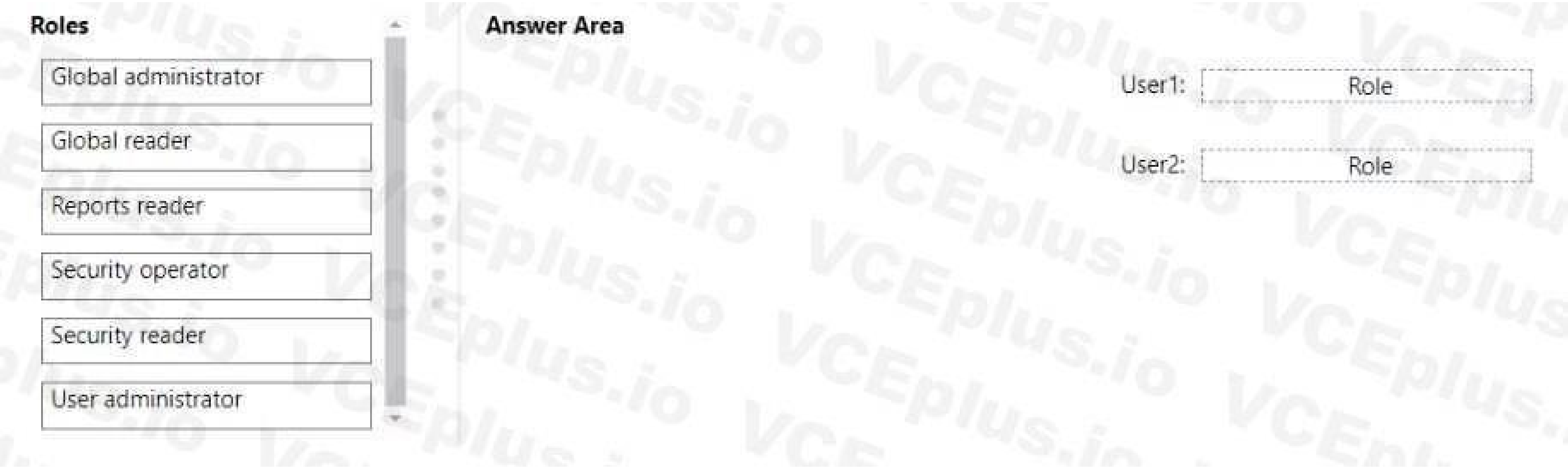
You have a Microsoft 365 E5 subscription that contains two users named User1 and User2.

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

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

NOTE: Each correct selection is worth one point.

Select and Place:



Roles

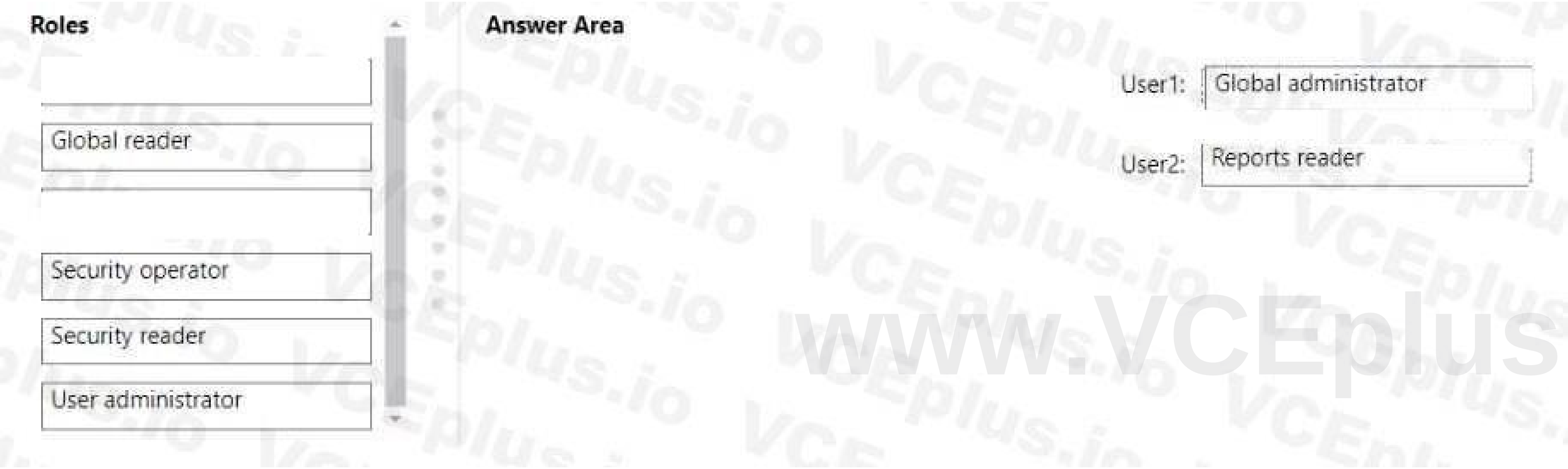
- Global administrator
- Global reader
- Reports reader
- Security operator
- Security reader
- User administrator

Answer Area

User1: Role

User2: Role

Correct Answer:



Roles

- Global reader
- Security operator
- Security reader
- User administrator

Answer Area

User1: Global administrator

User2: Reports reader

Section:
Explanation:

QUESTION 4

HOTSPOT

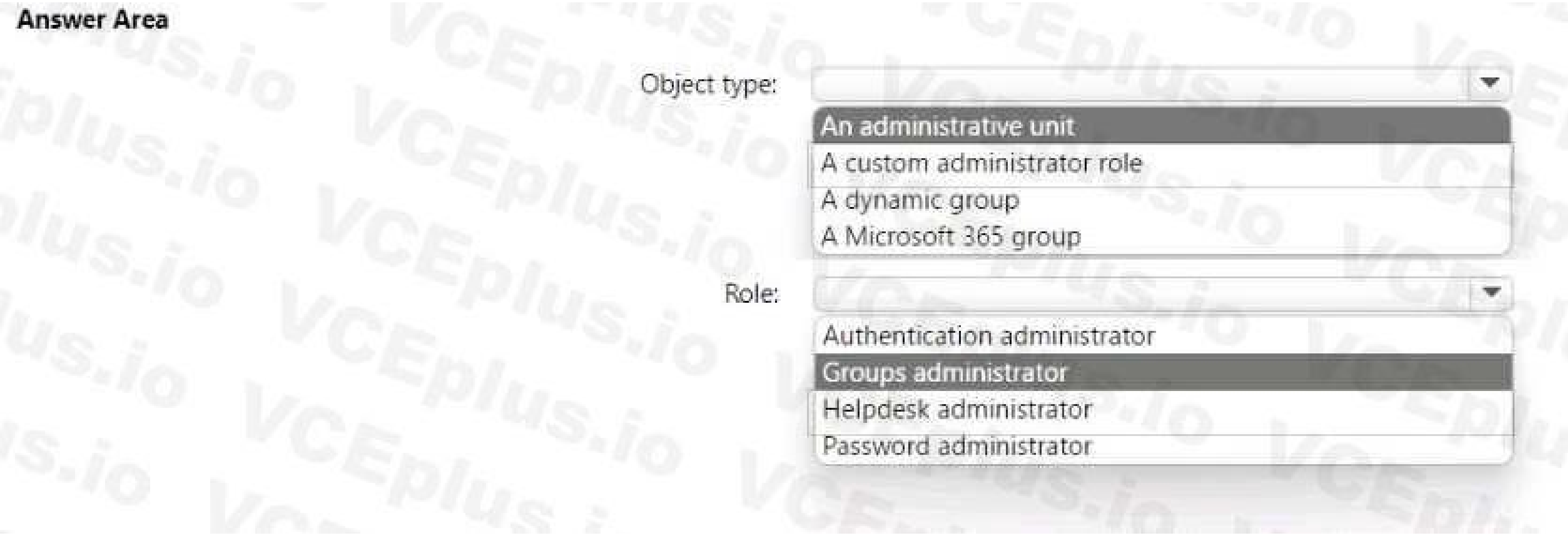
You have a Microsoft 365 tenant that has 5,000 users. One hundred of the users are executives. The executives have a dedicated support team.

You need to ensure that the support team can reset passwords and manage multi-factor authentication (MFA) settings for only the executives. The solution must use the principle of least privilege.

Which object type and Azure Active Directory (Azure AD) role should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

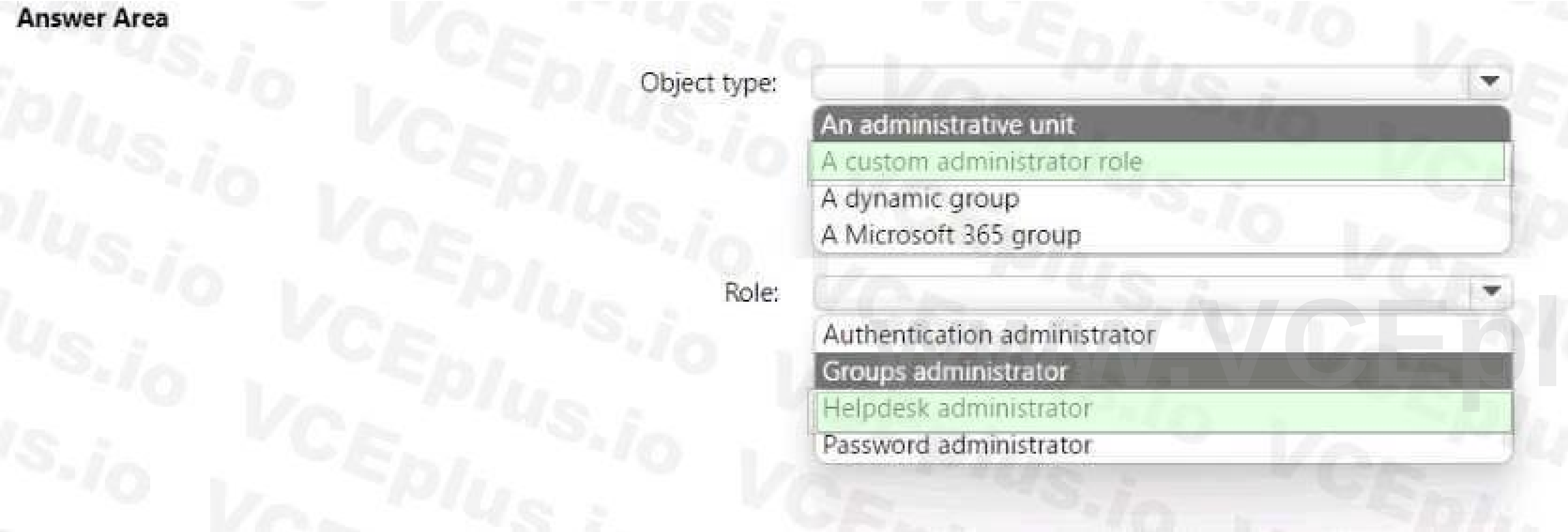
Object type:

- An administrative unit
- A custom administrator role
- A dynamic group
- A Microsoft 365 group

Role:

- Authentication administrator
- Groups administrator
- Helpdesk administrator
- Password administrator

Answer Area:



Answer Area

Object type:

- An administrative unit
- A custom administrator role
- A dynamic group
- A Microsoft 365 group

Role:

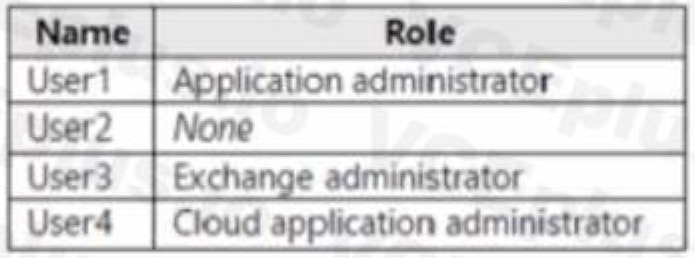
- Authentication administrator
- Groups administrator
- Helpdesk administrator
- Password administrator

Section:

Explanation:

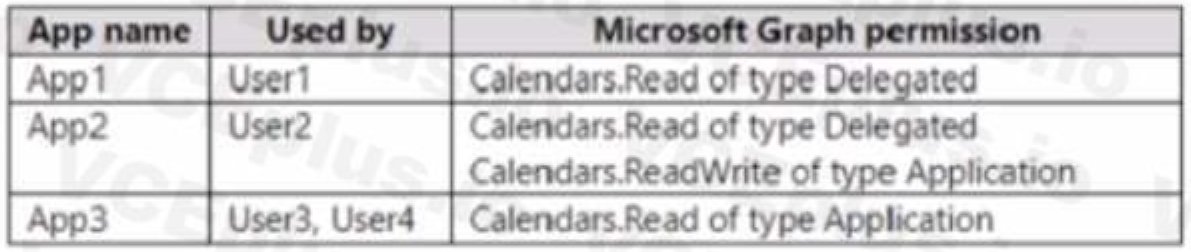
QUESTION 5

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



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

You have the app registrations shown in the following table.



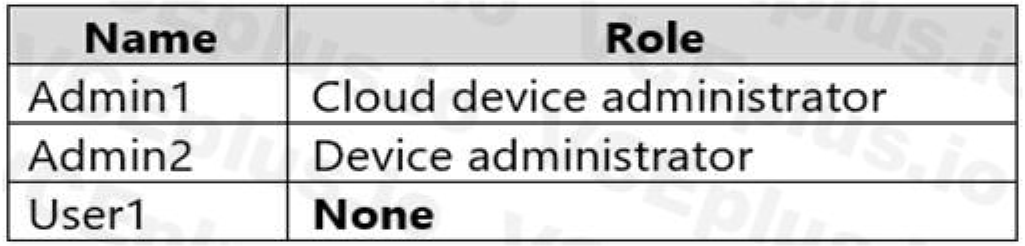
App name	Used by	Microsoft Graph permission
App1	User1	Calendars.Read of type Delegated
App2	User2	Calendars.Read of type Delegated Calendars.ReadWrite of type Application
App3	User3, User4	Calendars.Read of type Application

A company policy prevents changes to user permissions.
Which user can create appointments in the calendar of each user at the company?

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

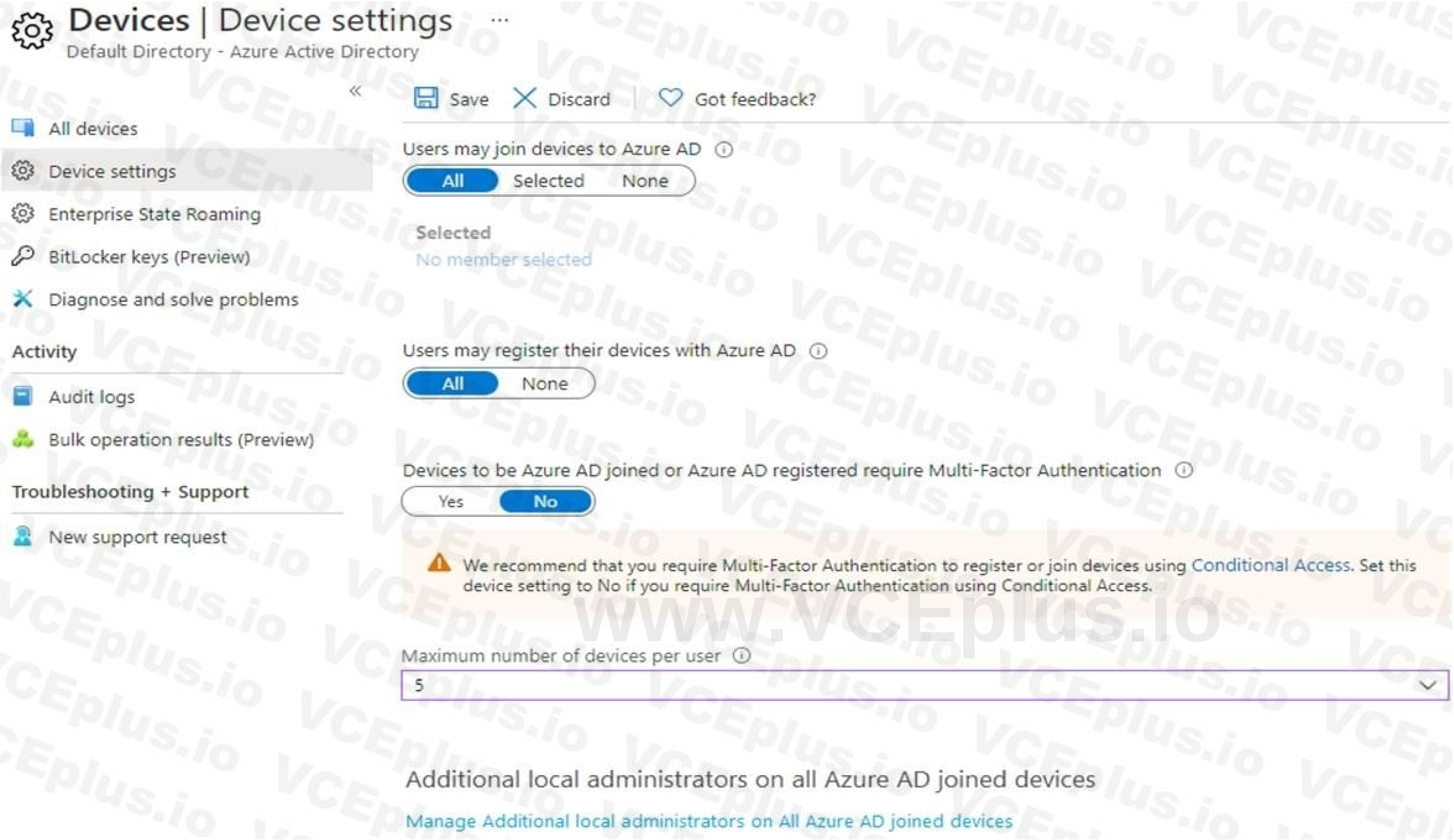
Correct Answer: C
Section:

QUESTION 6
HOTSPOT
You have an Azure Active Directory (Azure AD) tenant that has an Azure Active Directory Premium Plan 2 license. The tenant contains the users shown in the following table.



Name	Role
Admin1	Cloud device administrator
Admin2	Device administrator
User1	**None**

You have the Device Settings shown in the following exhibit.



Devices | Device settings ...

Default Directory - Azure Active Directory

Users may join devices to Azure AD ⓘ
[✓ All] Selected None

Selected
No member selected

Users may register their devices with Azure AD ⓘ
[✓ All] None

Devices to be Azure AD joined or Azure AD registered require Multi-Factor Authentication ⓘ
Yes [✓ No]

⚠ We recommend that you require Multi-Factor Authentication to register or join devices using Conditional Access. Set this device setting to No if you require Multi-Factor Authentication using Conditional Access.

Maximum number of devices per user ⓘ
5

Additional local administrators on all Azure AD joined devices

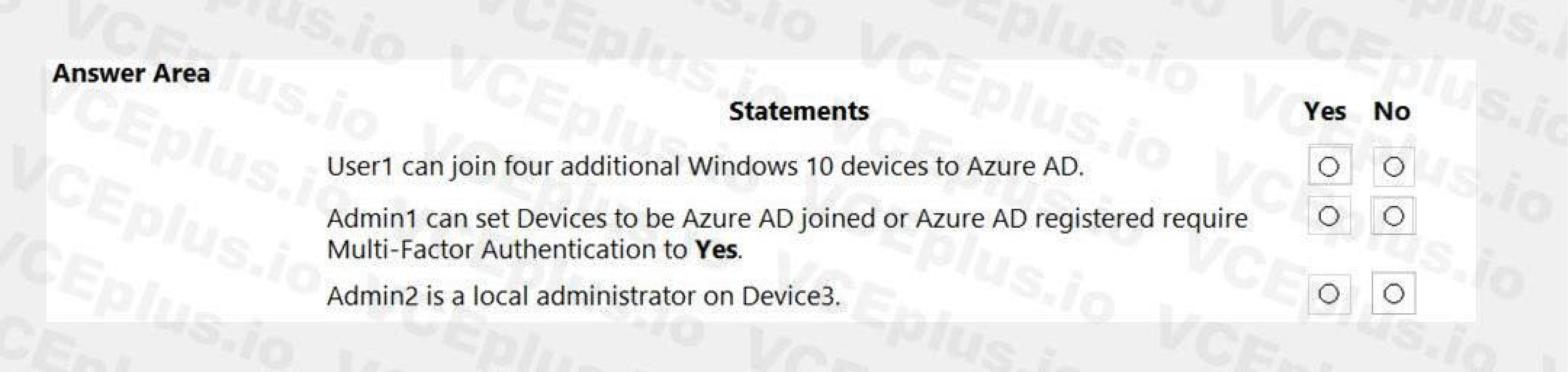
Manage Additional local administrators on All Azure AD joined devices

User1 has the devices shown in the following table.

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

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

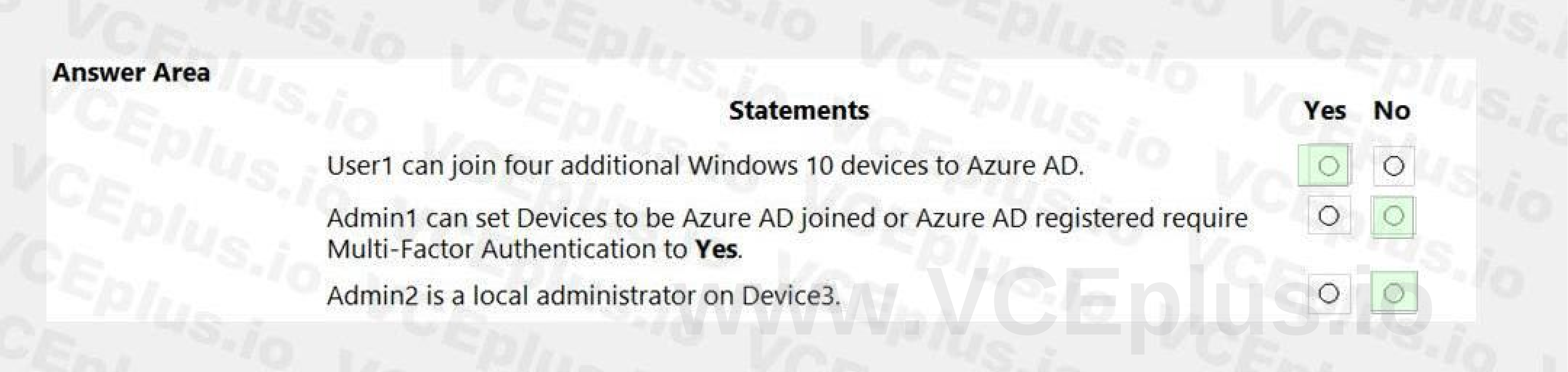
Hot Area:



Answer Area

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

Answer Area:



Answer Area

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

Section:

Explanation:

Box 1: Yes

Users may join 5 devices to Azure AD.

Box 2: No

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

Box 3: No

An additional local device administrator has not been applied

Reference:

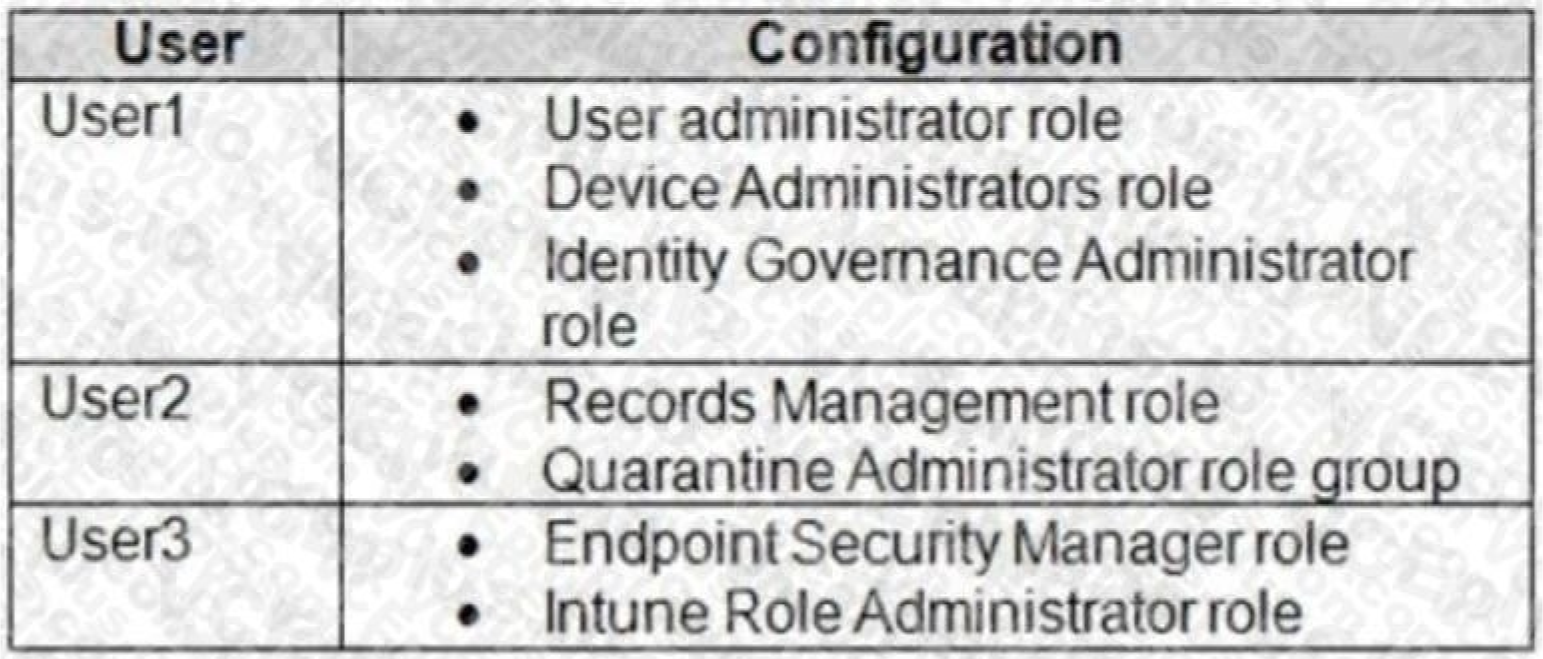
https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal

QUESTION 7

DRAG DROP

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

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

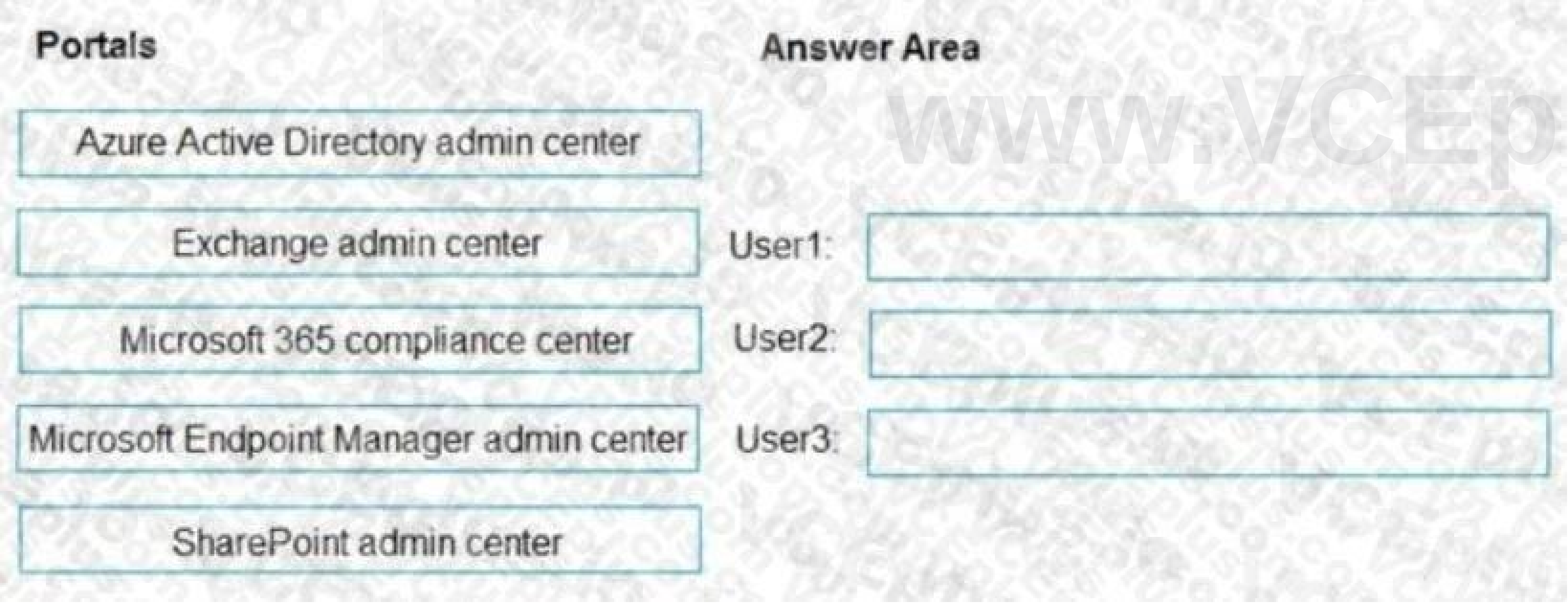


User	Configuration
User1	- User administrator role - Device Administrators role - Identity Governance Administrator role
User2	- Records Management role - Quarantine Administrator role group
User3	- Endpoint Security Manager role - Intune Role Administrator role

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

NOTE: Each correct selection is worth one point.

Select and Place:



Portals

- Azure Active Directory admin center
- Exchange admin center
- Microsoft 365 compliance center
- Microsoft Endpoint Manager admin center
- SharePoint admin center

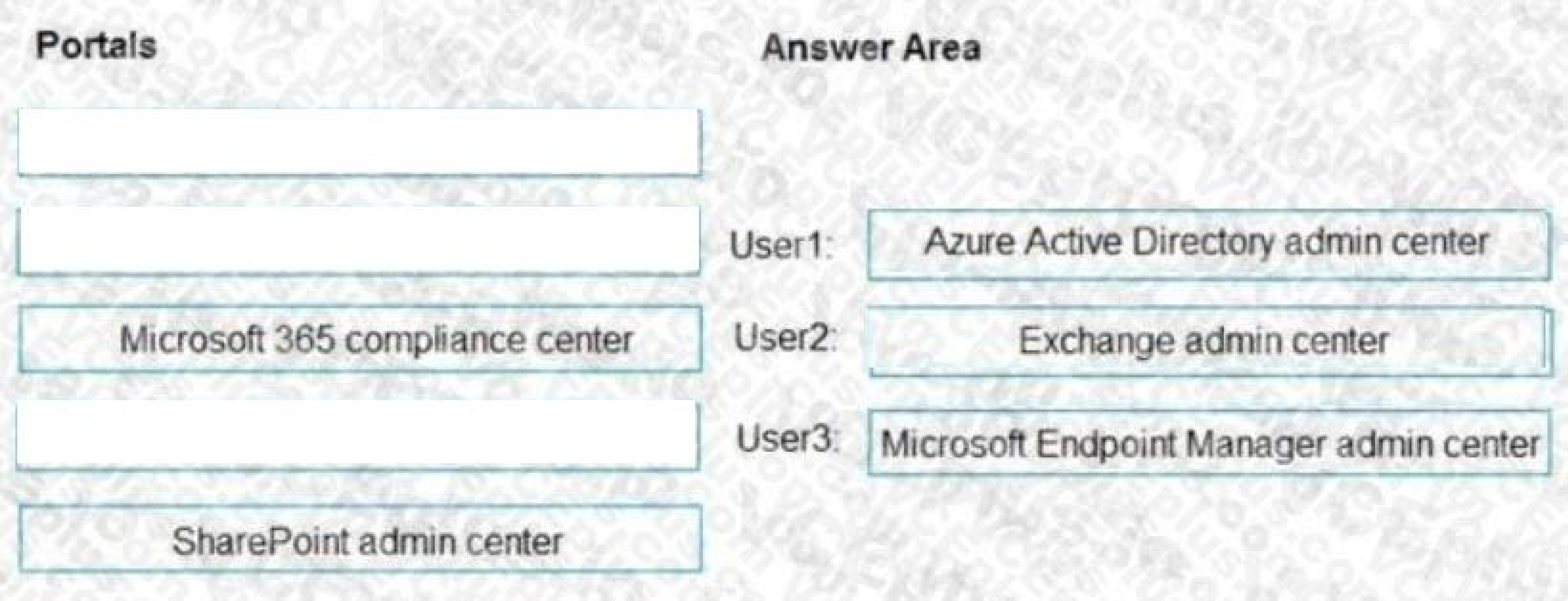
Answer Area

User1:

User2:

User3:

Correct Answer:



Portals

Microsoft 365 compliance center

SharePoint admin center

Answer Area

User1: Azure Active Directory admin center

User2: Exchange admin center

User3: Microsoft Endpoint Manager admin center

Section:
Explanation:

QUESTION 8
You have a Microsoft 365 E5 subscription.
You need to create a Microsoft Defender for Cloud Apps session policy.
What should you do first?

A. From the Microsoft Defender for Cloud Apps portal, select User monitoring.
B. From the Microsoft Defender for Cloud Apps portal, select App onboarding/maintenance
C. From the Azure Active Directory admin center, create a Conditional Access policy.
D. From the Microsoft Defender for Cloud Apps portal, create a continuous report.

Correct Answer: A
Section:

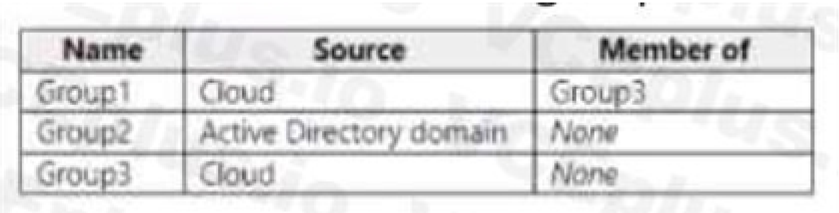
QUESTION 9
You need to meet the authentication requirements for leaked credentials.
What should you do?

A. Enable federation with PingFederate in Azure AD Connect.
B. Configure Azure AD Password Protection.
C. Enable password hash synchronization in Azure AD Connect.
D. Configure an authentication method policy in Azure AD.

Correct Answer: C
Section:
Explanation:
https://docs.microsoft.com/en-us/azure/security/fundamentals/steps-secure-identity

QUESTION 10
HOTSPOT

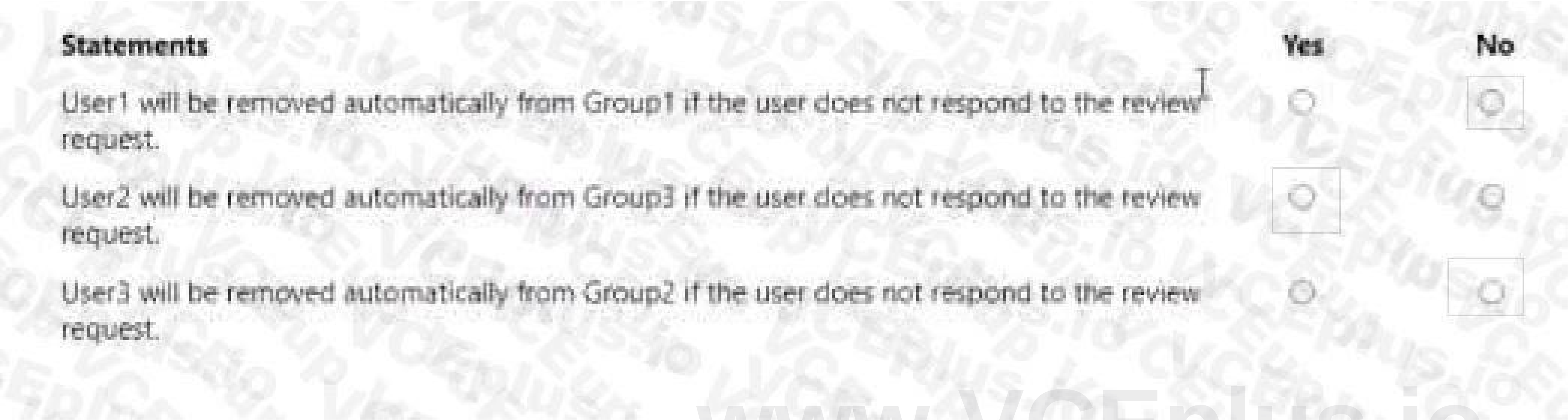
Your network contains an on-premises Active Directory domain that syncs to an Azure Active Directory (Azure AD) tenant.
The tenant contains the groups shown in the following table.



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

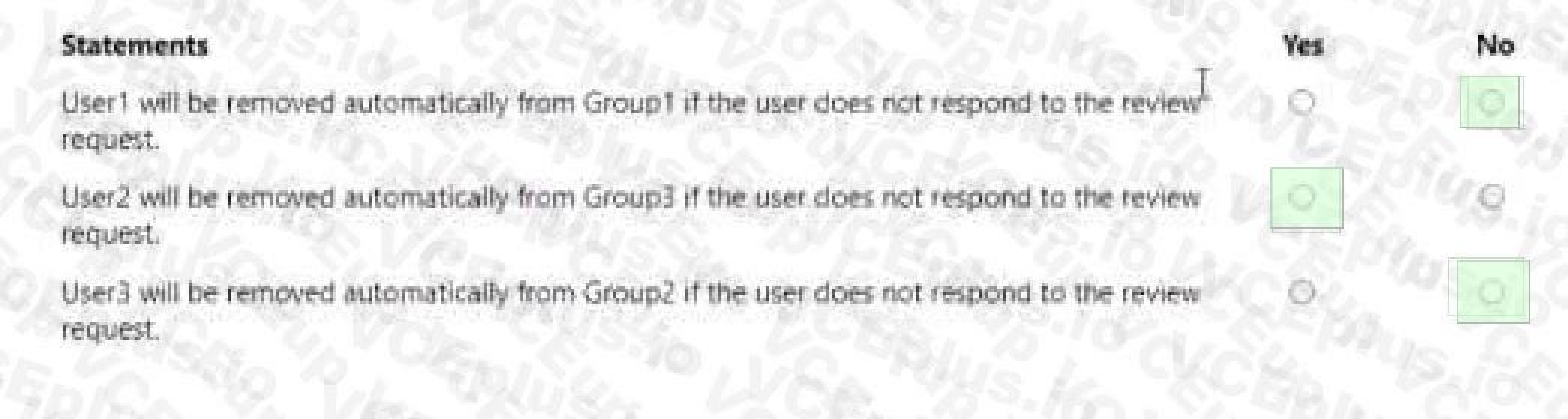
The tenant contains the users shown in the following table.

Hot Area:



Statements	Yes	No
User1 will be removed automatically from Group1 if the user does not respond to the review request.	○	○
User2 will be removed automatically from Group3 if the user does not respond to the review request.	○	○
User3 will be removed automatically from Group2 if the user does not respond to the review request.	○	○

Answer Area:



Statements	Yes	No
User1 will be removed automatically from Group1 if the user does not respond to the review request.	○	[✓ ○]
User2 will be removed automatically from Group3 if the user does not respond to the review request.	[✓ ○]	○
User3 will be removed automatically from Group2 if the user does not respond to the review request.	○	[✓ ○]

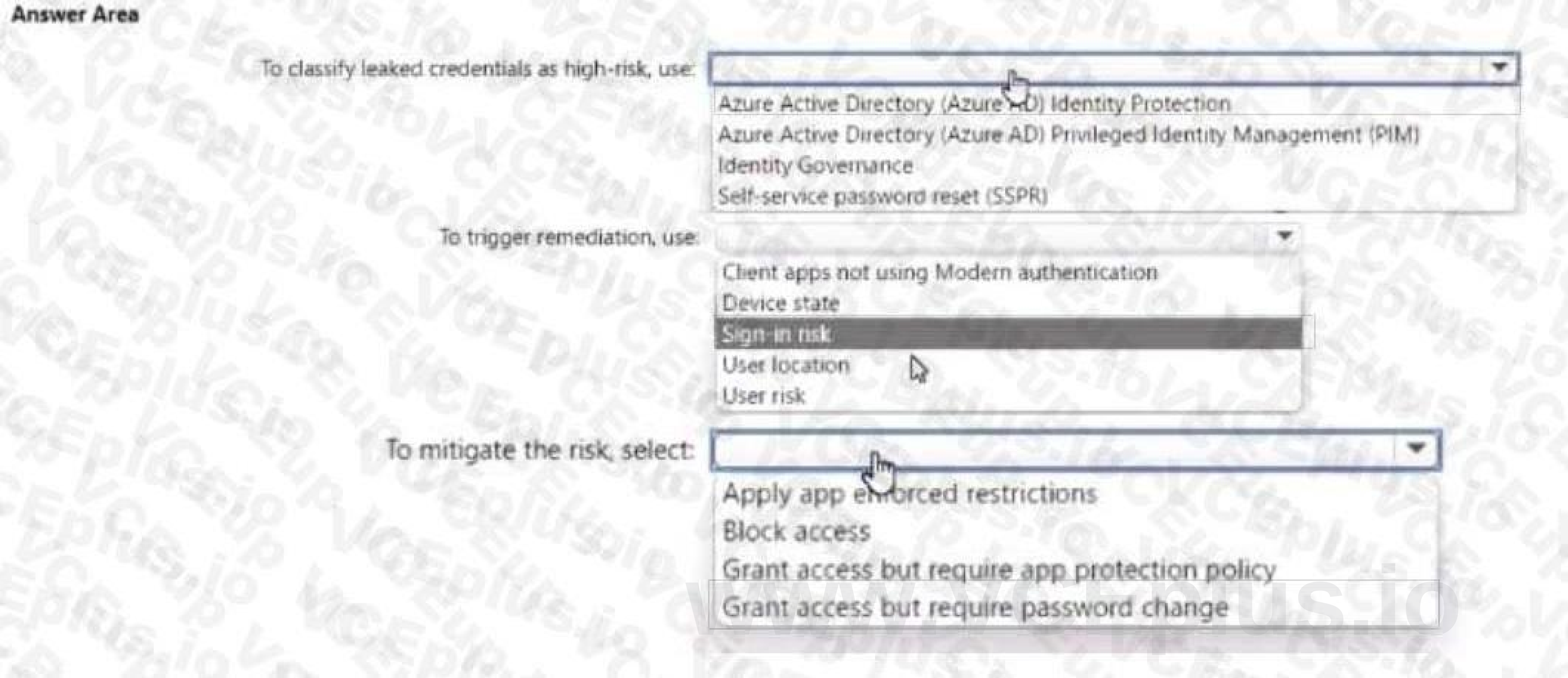
Section:
Explanation:

QUESTION 11
HOTSPOT
You have a Microsoft 365 tenant.
You need to Identity users who have leaked credentials. The solution must meet the following requirements:

- Identity sign-ms 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 m the answer area.

Hot Area:



Answer Area

To classify leaked credentials as high-risk, use:

- Azure Active Directory (Azure AD) Identity Protection
- Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
- Identity Governance
- Self-service password reset (SSPR)

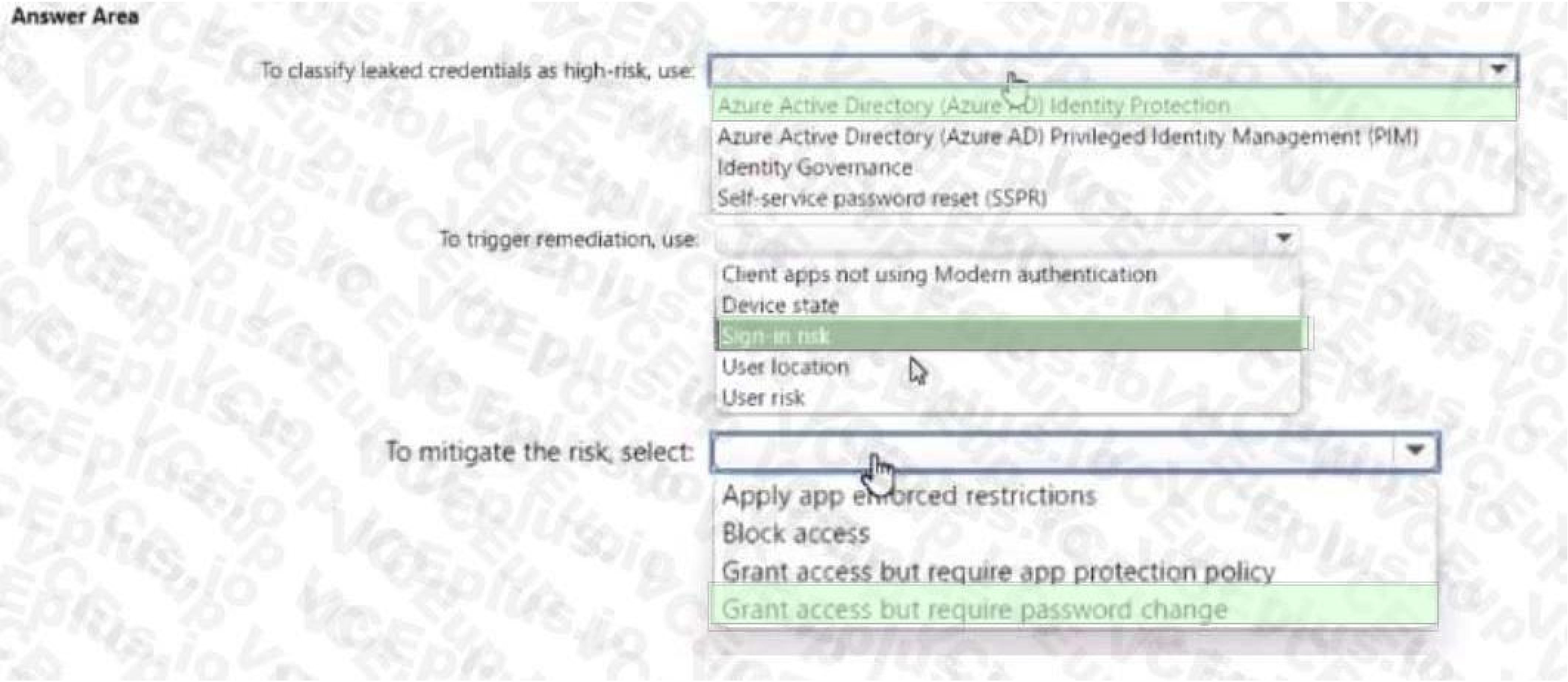
To trigger remediation, use:

- Client apps not using Modern authentication
- Device state
- Sign-in risk
- User location
- User risk

To mitigate the risk, select:

- Apply app enforced restrictions
- Block access
- Grant access but require app protection policy
- Grant access but require password change

Answer 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

Section:
Explanation:

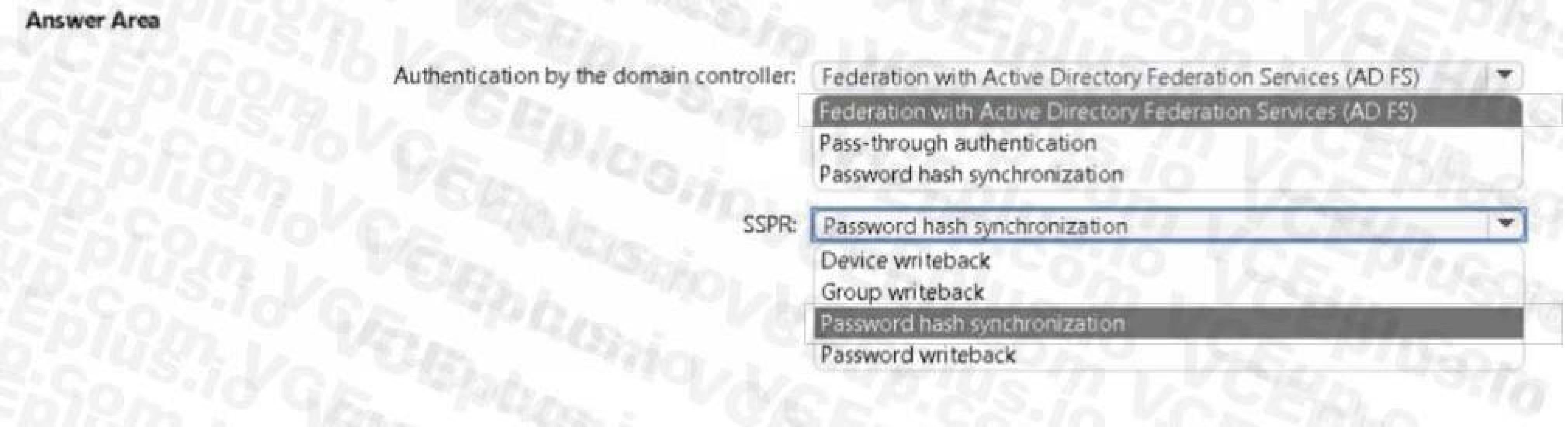
QUESTION 12
You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site!. Site! hosts PDF files
You need to prevent users from printing the files directly from Sitel.
Which type of policy should you create in the Microsoft Defender for Cloud Apps portal?

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

Correct Answer: D
Section:

QUESTION 13
HOTSPOT
Your on-premises network contains an Active Directory domain that uses Azure AD Connect to sync with an Azure AD tenant. You need to configure Azure AD Connect to meet the following requirements:
• User sign-ins to Azure AD must be authenticated by an Active Directory domain controller.
• Active Directory domain users must be able to use Azure AD self-service password reset (SSPR).
What should you use for each requirement? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

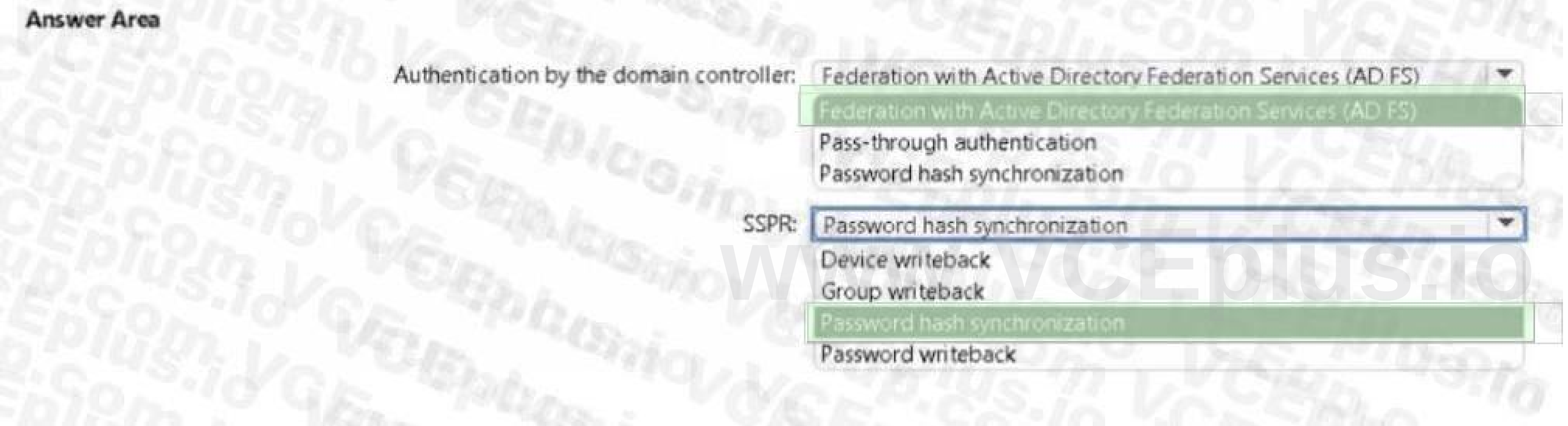
Authentication by the domain controller: Federation with Active Directory Federation Services (AD FS)

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

SSPR: Password hash synchronization

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

Answer Area:



Answer Area

Authentication by the domain controller: Federation with Active Directory Federation Services (AD FS)

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

SSPR: Password hash synchronization

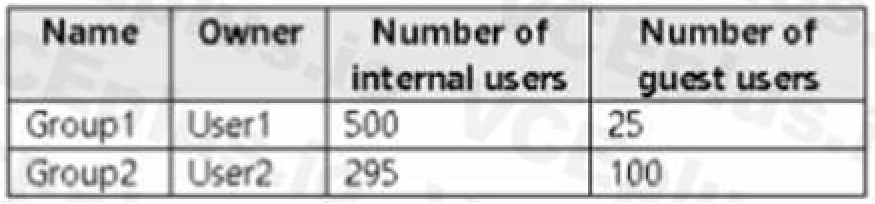
- Device writeback
- Group writeback
- Password hash synchronization
- Password writeback

Section:
Explanation:

QUESTION 14

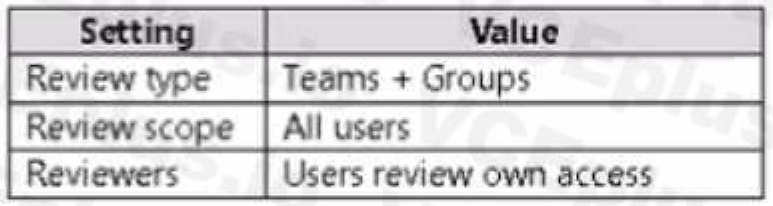
HOTSPOT

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



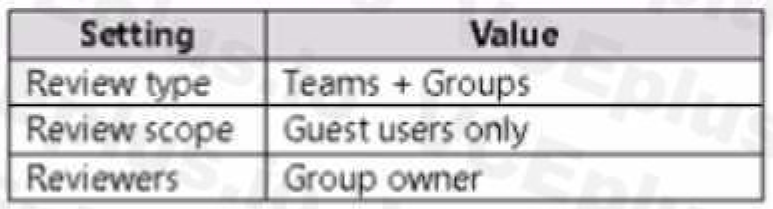
Name	Owner	Number of internal users	Number of guest users
Group1	User1	500	25
Group2	User2	295	100

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



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

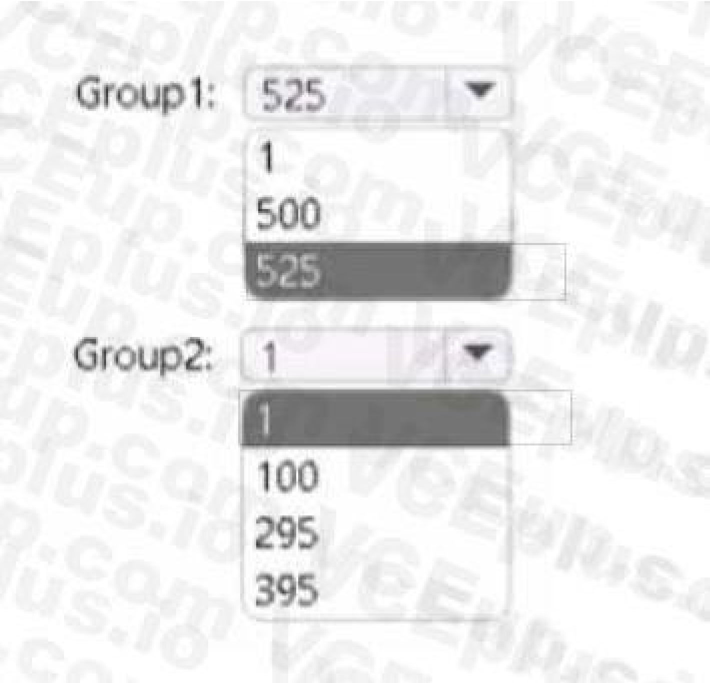
You create an access review for Group2 as shown in the following table.



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

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

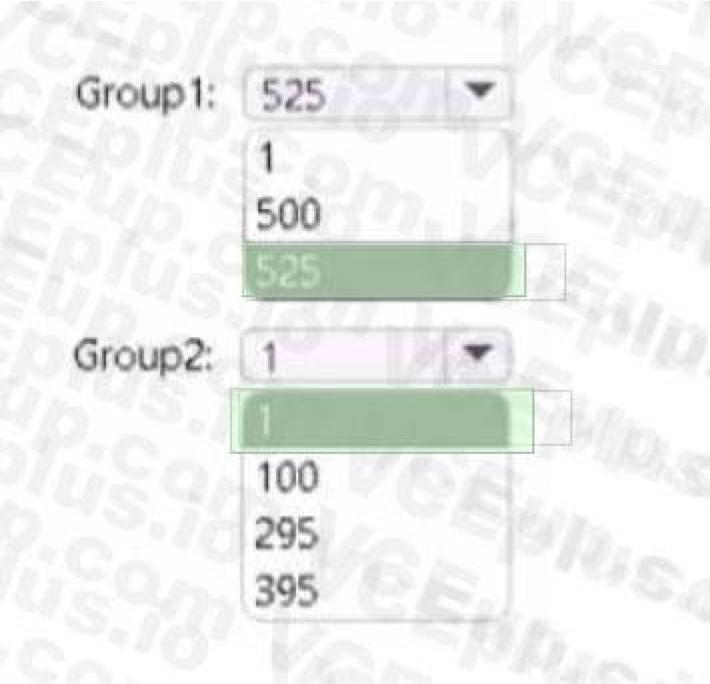
Hot Area:



Group1: 525
- 1
- 500
- 525

Group2: 1
- 1
- 100
- 295
- 395

Answer Area:



Group1: 525
- 1
- 500
- [✓ 525]

Group2: 1
- [✓ 1]
- 100
- 295
- 395

Section:
Explanation:

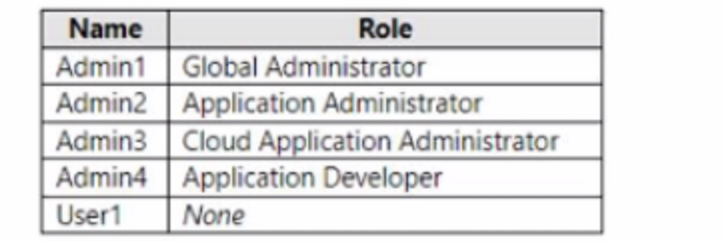
QUESTION 15

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

A. password spray
B. anonymous IP address
C. unfamiliar sign-in properties
D. Azure AD threat intelligence

Correct Answer: A
Section:

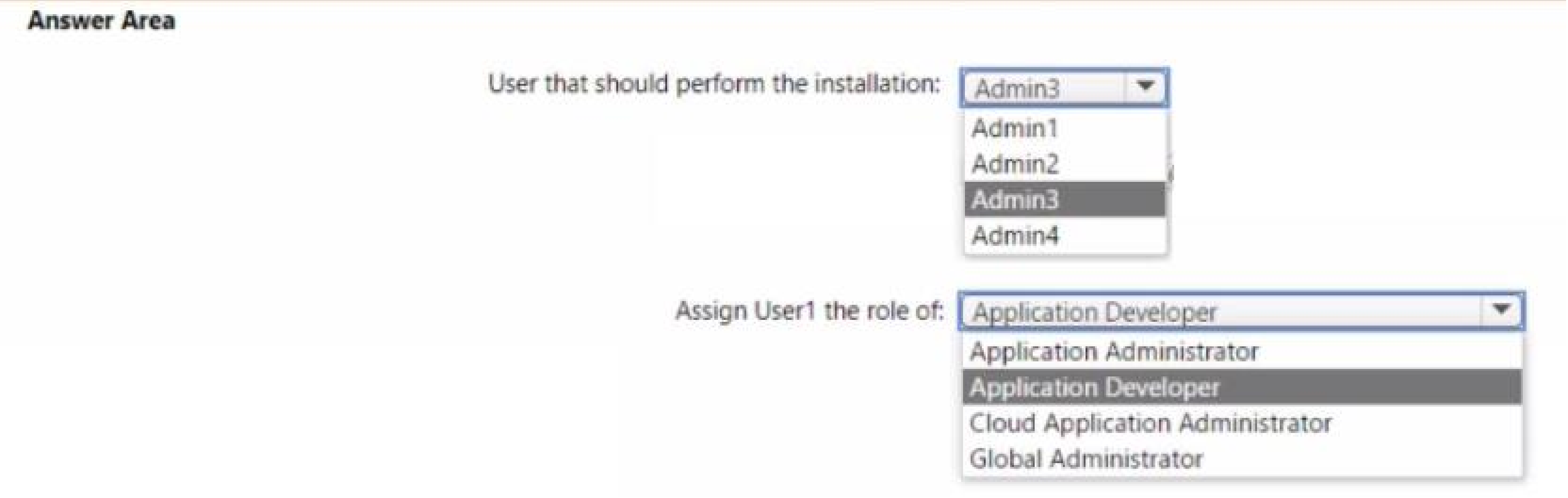
QUESTION 16
HOTSPOT
You have a hybrid Microsoft 365 subscription that contains the users show in the following table.



Name	Role
Admin1	Global Administrator
Admin2	Application Administrator
Admin3	Cloud Application Administrator
Admin4	Application Developer
User1	*None*

You plan to deploy an on-premises app1. App1 will be registered in Azure AD and will use Azure AD Application Proxy.
You need to delegate the installation of the Application Proxy connector and ensure that User1 can register App1 in Azure AD. The solution must use the principle of least privilege.
Which user should perform the installation, and which role should you assign to Users1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:

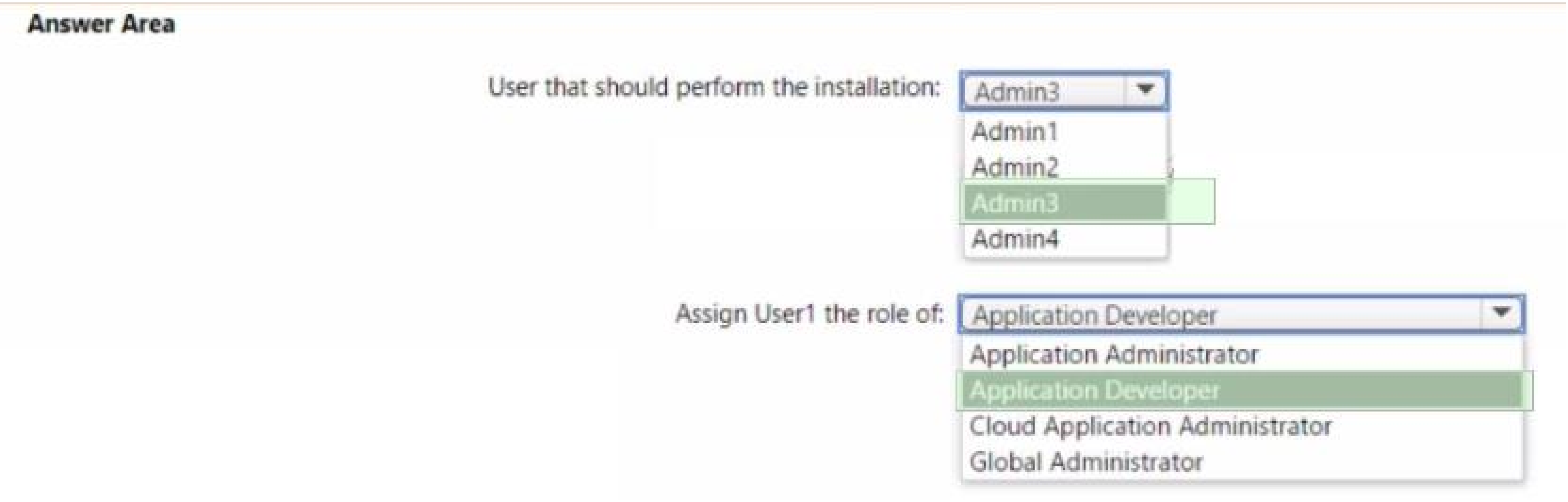


Answer Area

User that should perform the installation: Admin3

Assign User1 the role of: Application Developer

Answer Area:



Answer Area

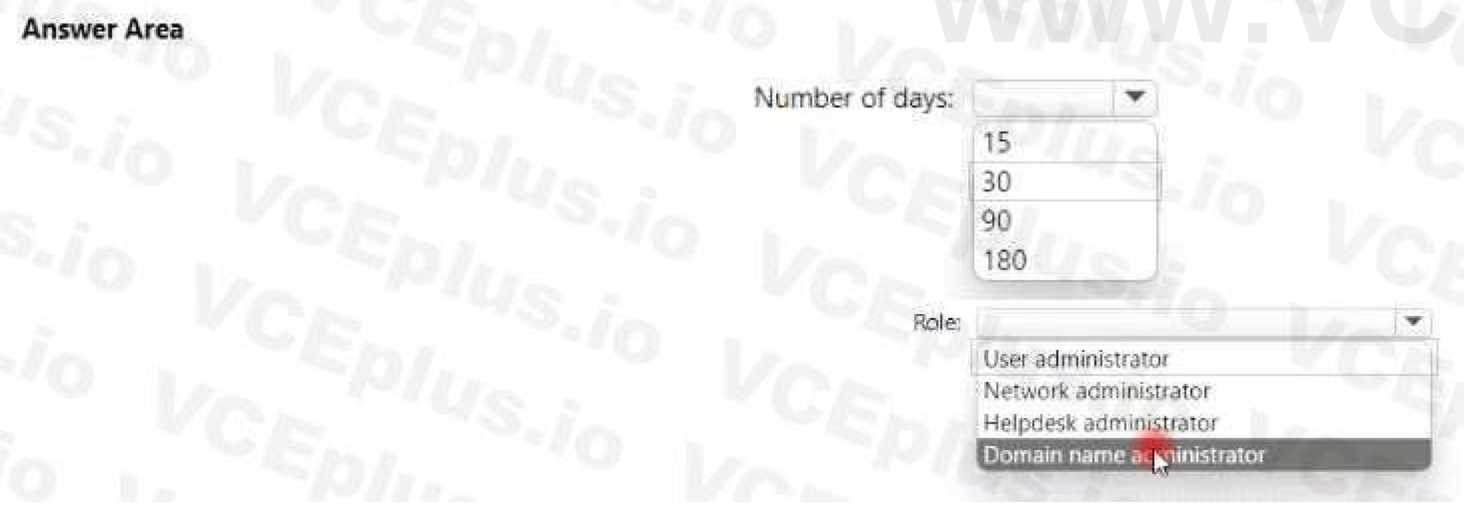
User that should perform the installation: Admin3

Assign User1 the role of: Application Developer

Section:
Explanation:

QUESTION 17
HOTSPOT
You have an Azure Active Directory (Azure AD) tenant that contains a user named User1. An administrator deletes User1. You need to identity the following:
• How many days after the account of User1 is deleted can you restore the account?
• Which is the least privileged role that can be used to restore User1?
What should you identify? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

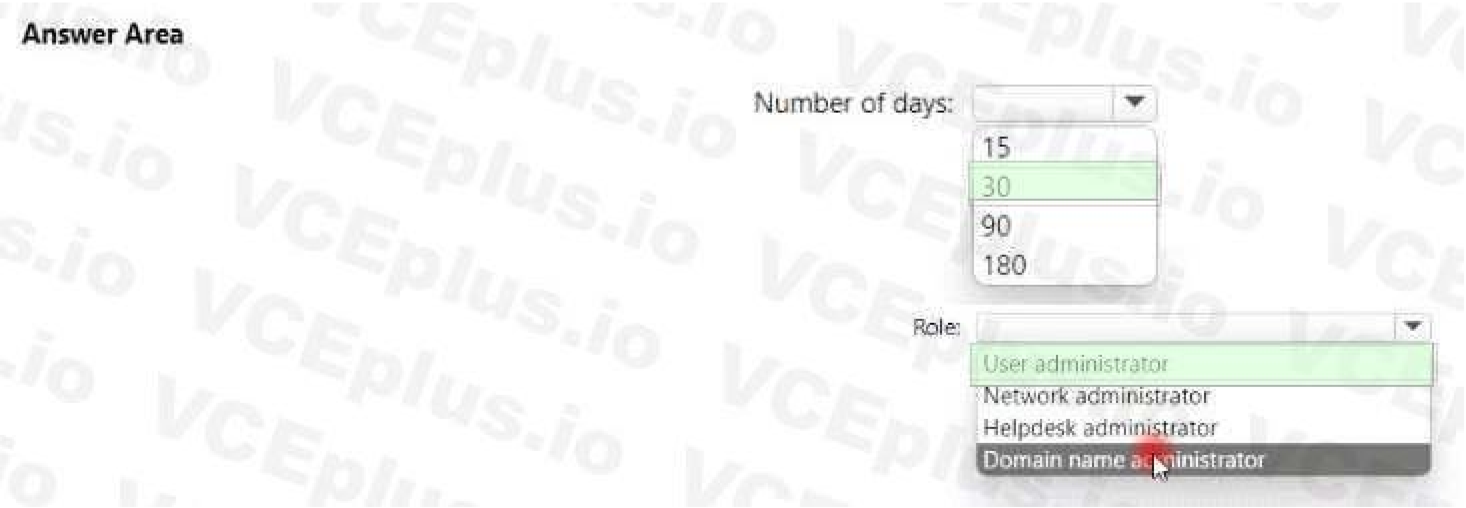


Answer Area

Number of days:

Role:

Answer Area:



Answer Area

Number of days:

- 15
- [✓ 30]
- 90
- 180

Role:

- [✓ User administrator]
- Network administrator
- Helpdesk administrator
- Domain name administrator

Section:
Explanation:

QUESTION 18
You use Azure Monitor to analyze Azure Active Directory (Azure AD) activity logs.
Yon receive more than 100 email alerts each day for tailed Azure Al) user sign-in attempts.
You need to ensure that a new security administrator receives the alerts instead of you.
Solution: From Azure monitor, you modify the action group.
Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section:

QUESTION 19
You use Azure Monitor to analyze Azure Active Directory (Azure AD) activity logs.
Yon receive more than 100 email alerts each day for tailed Azure Al) user sign-in attempts.
You need to ensure that a new security administrator receives the alerts instead of you.
Solution: From Azure monitor, you create a data collection rule.
Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section:

QUESTION 20
You have a Microsoft 365 tenant.
All users must use the Microsoft Authenticator app for multi-factor authentication (MFA) when accessing Microsoft 365 services.
Some users report that they received an MFA prompt on their Microsoft Authenticator app without initiating a sign-in request.
You need to block the users automatically when they report an MFA request that they did not Initiate.
Solution: From the Azure portal, you configure the Block/unblock users settings for multi-factor authentication (MFA).
Does this meet the goal?

A. Yes

B. No

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

QUESTION 21
You have a Microsoft 365 tenant.
All users must use the Microsoft Authenticator app for multi-factor authentication (MFA) when accessing Microsoft 365 services.
Some users report that they received an MFA prompt on their Microsoft Authenticator app without initiating a sign-in request.
You need to block the users automatically when they report an MFA request that they did not Initiate.
Solution: From the Azure portal, you configure the Account lockout settings for multi-factor authentication (MFA).
Does this meet the goal?

A. Yes

B. No

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

QUESTION 22
You have a Microsoft 365 tenant.
All users must use the Microsoft Authenticator app for multi-factor authentication (MFA) when accessing Microsoft 365 services.
Some users report that they received an MFA prompt on their Microsoft Authenticator app without initiating a sign-in request.
You need to block the users automatically when they report an MFA request that they did not Initiate.
Solution: From the Azure portal, you configure the Fraud alert settings for multi-factor authentication (MFA).
Does this meet the goal?

A. Yes

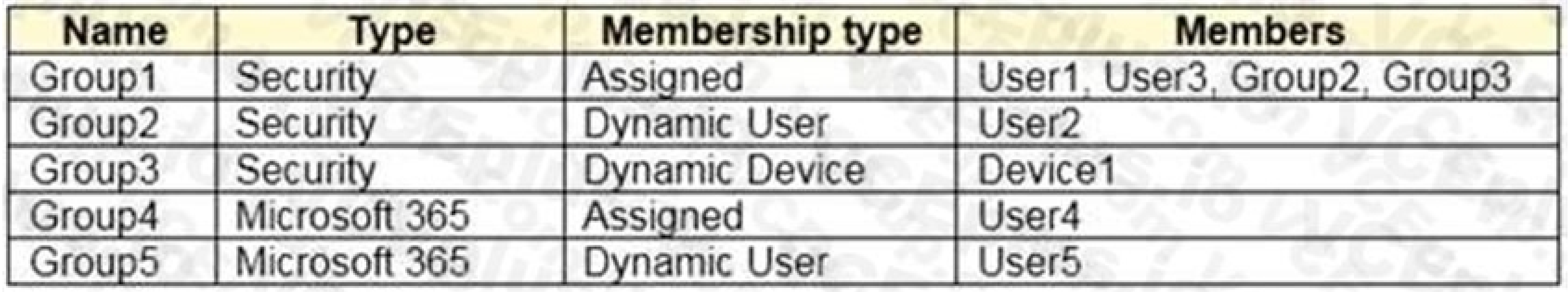
B. No

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

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

QUESTION 23

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



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

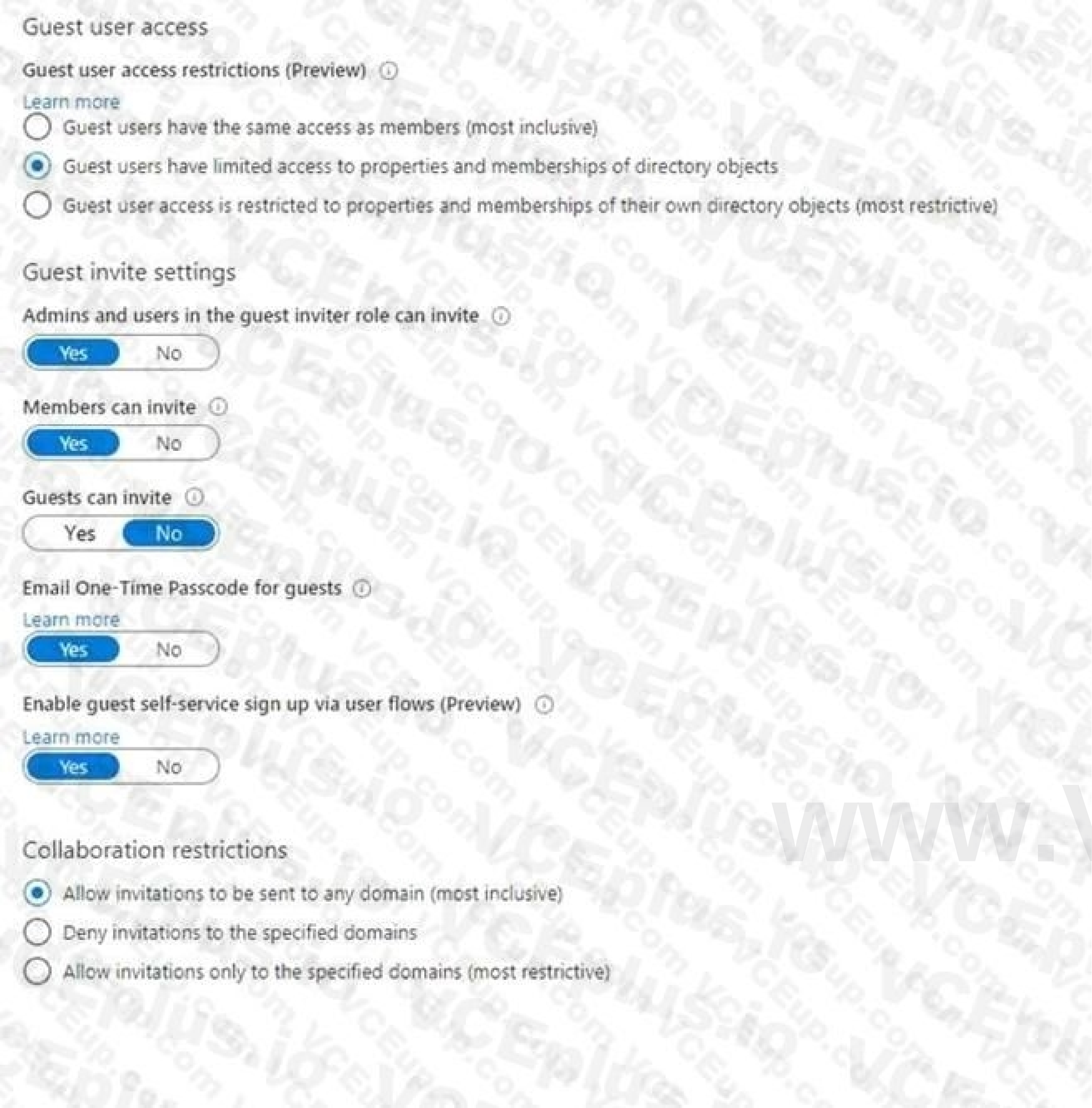
To which groups can you assign a Microsoft Office 365 Enterprise E5 license directly?

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

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

QUESTION 24

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

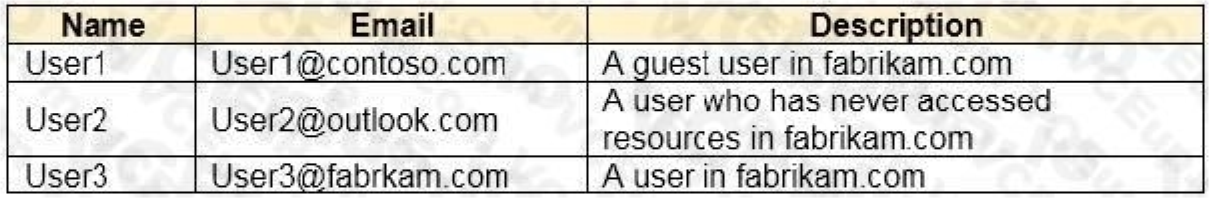
Collaboration restrictions

● 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

Correct Answer: A

Section:

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

QUESTION 25
You have 2,500 users who are assigned Microsoft Office 365 Enterprise E3 licenses. The licenses are assigned to individual users.
From the Groups blade in the Azure Active Directory admin center, you assign Microsoft 365 Enterprise E5 licenses to the users.
You need to remove the Office 365 Enterprise E3 licenses from the users by using the least amount of administrative effort.
What should you use?

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

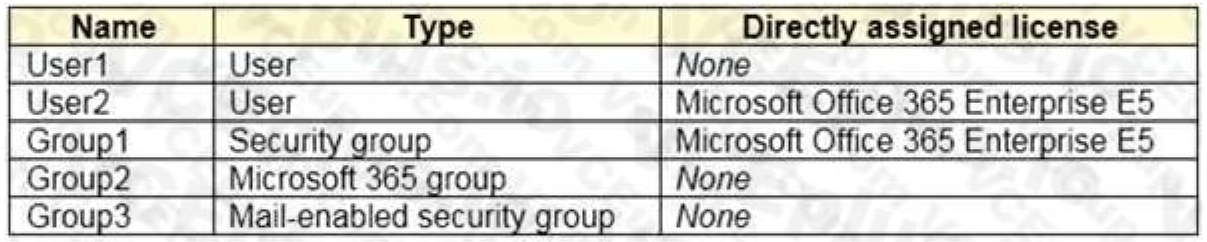
Correct Answer: C
Section:

QUESTION 26
You have an Azure Active Directory (Azure AD) tenant named contoso.com.
You plan to bulk invite Azure AD business-to-business (B2B) collaboration users.
Which two parameters must you include when you create the bulk invite? Each correct answer presents part of the solution NOTE: Each correct selection is worth one point.

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

Correct Answer: A, B
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/tutorial-bulk-invite

QUESTION 27
You have an Azure Active Directory (Azure AD) tenant that contains the objects shown in the following table.



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

Which objects can you add as members to Group3?

A. User2 and Group2 only
B. User2, Group1, and Group2 only
C. User1, User2, Group1 and Group2

D. User1 and User2 only

E. User2 only

Correct Answer: E
Section:
Explanation:
Reference:
https://bitsizedbytes.wordpress.com/2018/12/10/distribution-security-and-office-365-groupsnesting/

QUESTION 28

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 password writeback.
Does this meet the goal?

A. Yes

B. No

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

QUESTION 29

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 pass-through authentication.
Does this meet the goal?

A. Yes

B. No

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

QUESTION 30

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one

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

A. Yes
B. No

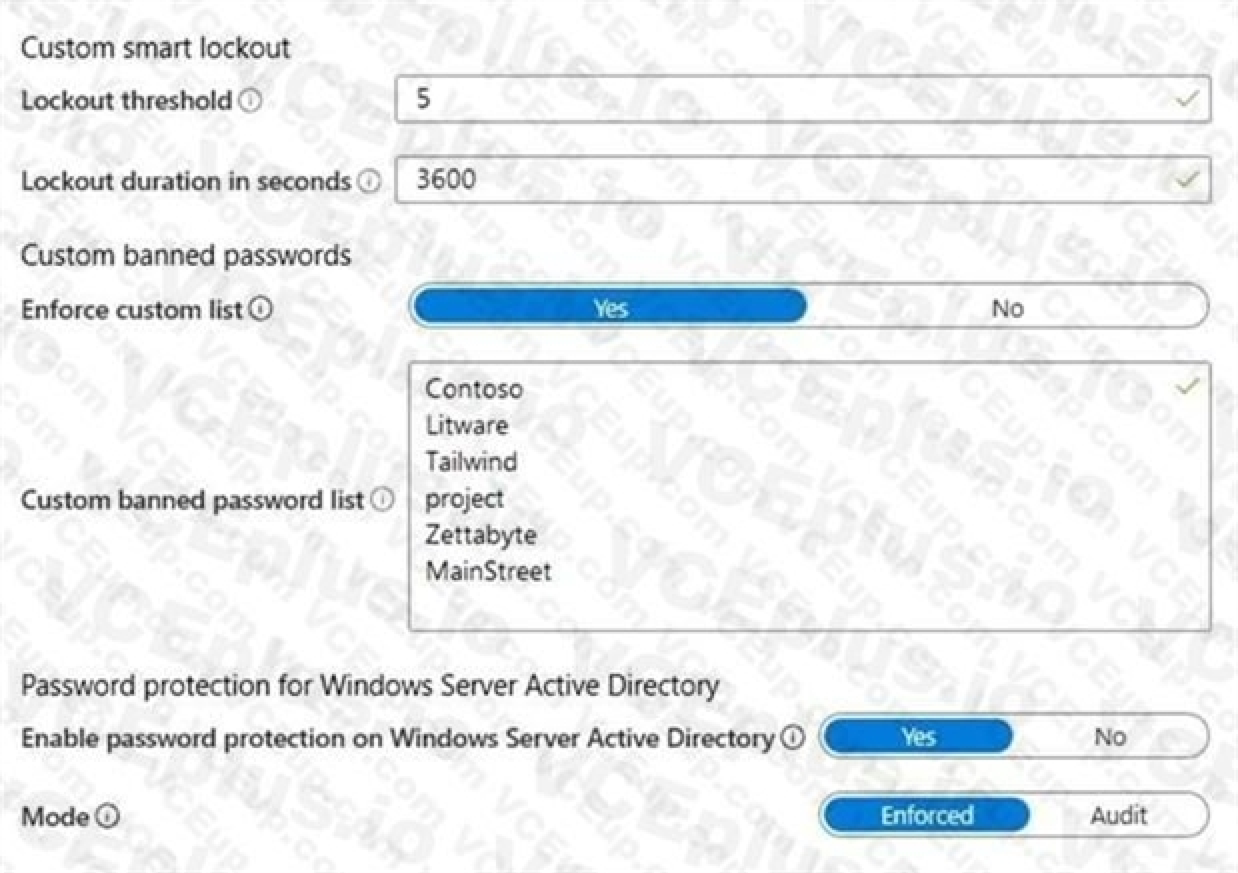
Correct Answer: B
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn

QUESTION 31
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 nonadministrative users. The solution must use the principle of least privilege.
Which role should you assign to SecAdmin1?

A. Authentication administrator
B. Helpdesk administrator
C. Privileged authentication administrator
D. Security operator

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

QUESTION 32
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

Correct Answer: C
Section:
Explanation:
Reference:
https://blog.enablingtechcorp.com/azure-ad-password-protection-password-evaluation

QUESTION 33
You have a Microsoft 365 tenant.
All users have mobile phones and laptops.
The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity.
While working from the remote locations, the users connect their laptop to a wired network that has internet access.
You plan to implement multi-factor authentication (MFA).
Which MFA authentication method can the users use from the remote location?

A. a verification code from the Microsoft Authenticator app

B. security questions
C. voice
D. an app password

Correct Answer: A
Section:
Explanation:

QUESTION 34
You configure a new Microsoft 365 tenant to use a default domain name of contoso.com.
You need to ensure that you can control access to Microsoft 365 resources by using conditional access policies.
What should you do first?

A. Disable the User consent settings.
B. Disable Security defaults.
C. Configure a multi-factor authentication (MFA) registration policy.
D. Configure password protection for Windows Server Active Directory.

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

QUESTION 35
Your company has a Microsoft 365 tenant.
The company has a call center that contains 300 users. In the call center, the users share desktop computers and might use a different computer every day. The call center computers are NOT configured for biometric identification.
The users are prohibited from having a mobile phone in the call center.
You need to require multi-factor authentication (MFA) for the call center users when they access Microsoft 365 services.
What should you include in the solution?

A. a named network location
B. the Microsoft Authenticator app
C. Windows Hello for Business authentication
D. FIDO2 tokens

Correct Answer: D
Section:
Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authenticationpasswordless

QUESTION 36
You have an Azure Active Directory (Azure AD) tenant named contoso.com.
All users who run applications registered in Azure AD are subject to conditional access policies.
You need to prevent the users from using legacy authentication.
What should you include in the conditional access policies to filter out legacy authentication attempts?

A. a cloud apps or actions condition
B. a user risk condition
C. a client apps condition
D. a sign-in risk condition

Correct Answer: C
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacyauthentication

QUESTION 37
You have an Azure Active Directory (Azure AD) tenant.
You open the risk detections report.
Which risk detection type is classified as a user risk?

A. impossible travel
B. anonymous IP address
C. atypical travel
D. leaked credentials

Correct Answer: D
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identityprotection-risks

QUESTION 38
You have a Microsoft 365 tenant.
All users have computers that run Windows 10. Most computers are company-owned and joined to Azure Active Directory (Azure AD). Some computers are user-owned and are only registered in Azure AD.
You need to prevent users who connect to Microsoft SharePoint Online on their user-owned computer from downloading or syncing files. Other users must NOT be restricted.
Which policy type should you create?

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

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

QUESTION 39
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

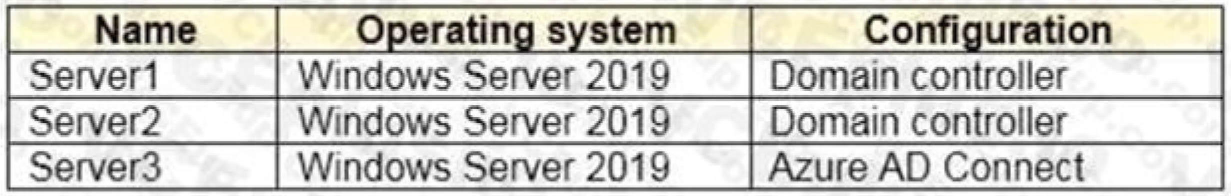
B. an Azure AD Password Protection proxy

C. Network Policy Server (NPS)

D. a pass-through authentication proxy

Correct Answer: C
Section:

QUESTION 40
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 2019	Domain controller
Server3	Windows Server 2019	Azure AD Connect

The domain controllers are prevented from communicating to the internet.
You implement Azure AD Password Protection on Server1 and Server2.
You deploy a new server named Server4 that runs Windows Server 2019.
You need to ensure that Azure AD Password Protection will continue to work if a single server fails.
What should you implement on Server4?

A. Azure AD Connect

B. Azure AD Application Proxy

C. Password Change Notification Service (PCNS)

D. the Azure AD Password Protection proxy service

Correct Answer: D
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-badon-premisesdeploy

QUESTION 41
You have a Microsoft 365 tenant.
The Azure Active Directory (Azure AD) tenant syncs to an on-premises Active Directory domain.
Users connect to the internet by using a hardware firewall at your company. The users authenticate to the firewall by using their Active Directory credentials.
You plan to manage access to external applications by using Azure AD.
You need to use the firewall logs to create a list of unmanaged external applications and the users who access them.
What should you use to gather the information?

A. Application Insights in Azure Monitor

B. access reviews in Azure AD

C. Cloud App Discovery in Microsoft Cloud App Security

D. enterprise applications in Azure AD

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

QUESTION 42
You have a Microsoft 365 tenant.
The Azure Active Directory (Azure AD) tenant syncs to an on-premises Active Directory domain.
You plan to create an emergency-access administrative account named Emergency1. Emergency1 will be assigned the Global administrator role in Azure AD. Emergency1 will be used in the event of Azure AD functionality failures and on- premises infrastructure failures.
You need to reduce the likelihood that Emergency1 will be prevented from signing in during an emergency.
What should you do?

A. Configure Azure Monitor to generate an alert if Emergency1 is modified or signs in.
B. Require Azure AD Privileged Identity Management (PIM) activation of the Global administrator role for Emergency1.
C. Configure a conditional access policy to restrict sign-in locations for Emergency1 to only the corporate network.
D. Configure a conditional access policy to require multi-factor authentication (MFA) for Emergency1.

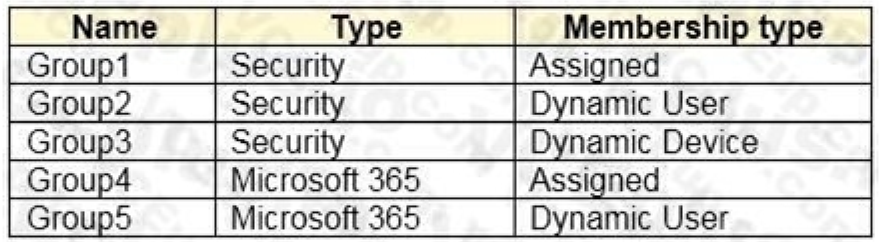
Correct Answer: A
Section:

QUESTION 43
You have a Microsoft 365 tenant.
In Azure Active Directory (Azure AD), you configure the terms of use.
You need to ensure that only users who accept the terms of use can access the resources in the tenant. Other users must be denied access.
What should you configure?

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

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

QUESTION 44
You have an Azure Active Directory (Azure AD) tenant that contains the groups shown in the following table.



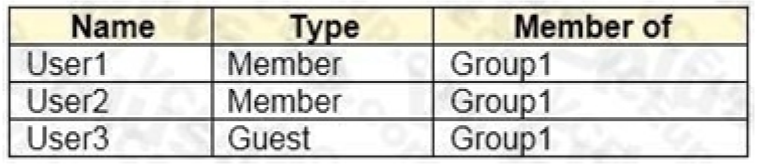
Name	Type	Membership type
Group1	Security	Assigned
Group2	Security	Dynamic User
Group3	Security	Dynamic Device
Group4	Microsoft 365	Assigned
Group5	Microsoft 365	Dynamic User

For which groups can you create an access review?

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

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

QUESTION 45
You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.



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

User1 is the owner of Group1.
You create an access review that has the following settings:
Users to review: Members of a group
Scope: Everyone
Group: Group1
Reviewers: Members (self)
Which users can perform access reviews for User3?

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

Correct Answer: B
Section:

QUESTION 46
Your company recently implemented Azure Active Directory (Azure AD) Privileged Identity Management (PIM).
While you review the roles in PIM, you discover that all 15 users in the IT department at the company have permanent security administrator rights.
You need to ensure that the IT department users only have access to the Security administrator role when required.
What should you configure for the Security administrator role assignment?

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

Correct Answer: D

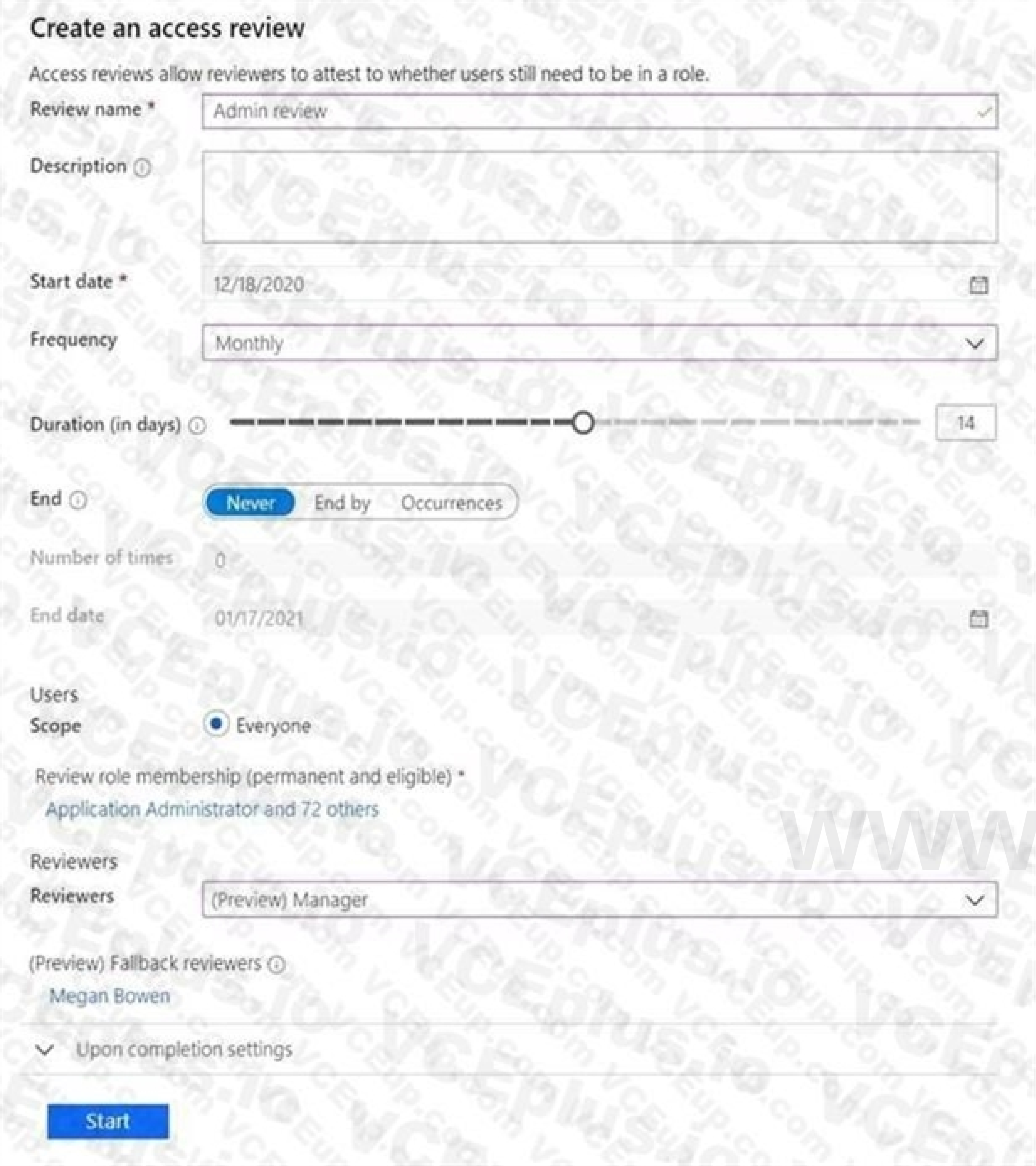
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pimconfigure

QUESTION 47
You have a Microsoft 365 tenant.
The Sign-ins activity report shows that an external contractor signed in to the Exchange admin center.
You need to review access to the Exchange admin center at the end of each month and block sign-ins if required.
What should you create?

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

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

QUESTION 48
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

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

A. Yes
B. No

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

QUESTION 49

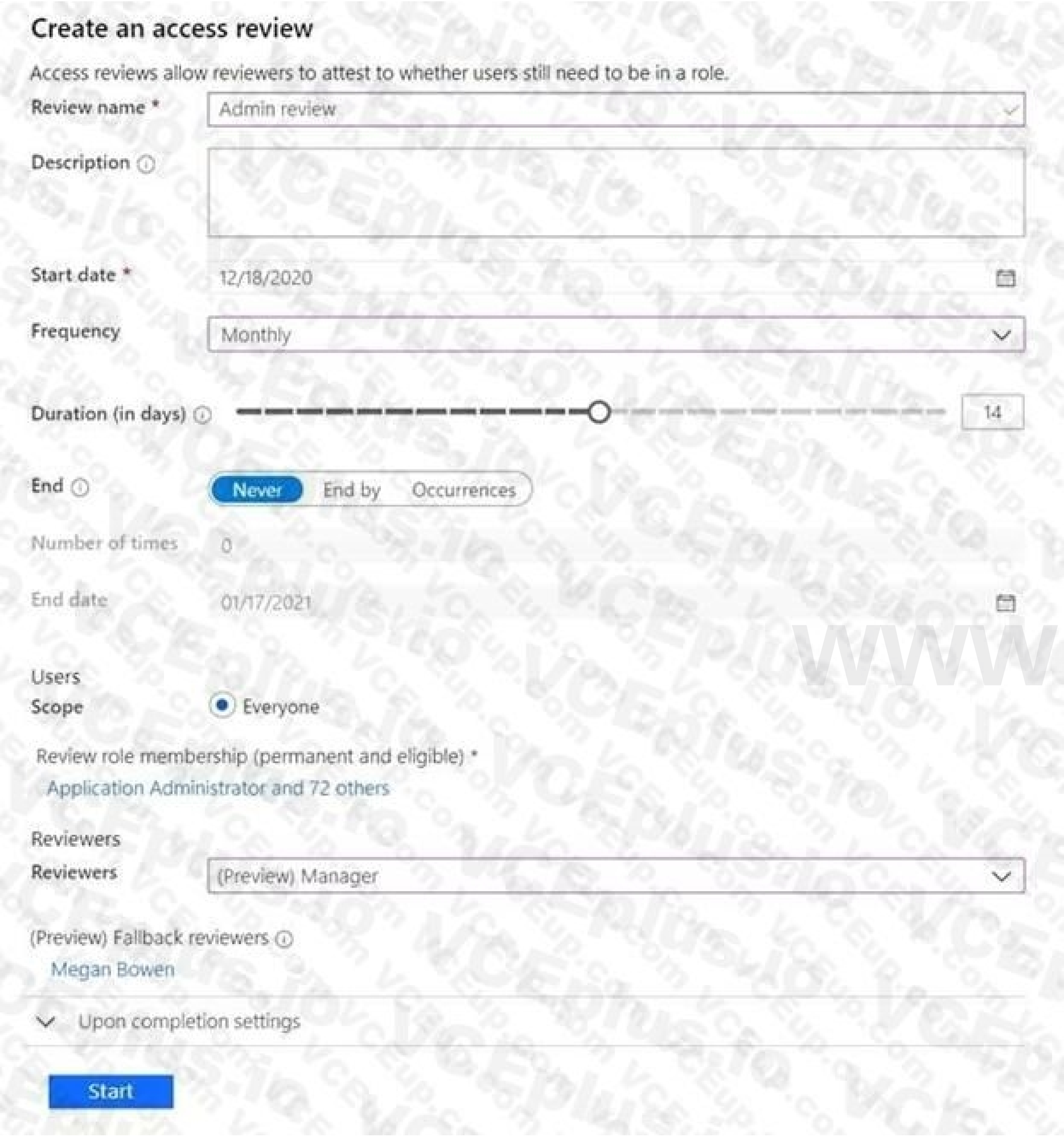
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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 modify the properties of the IT administrator user accounts.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

Section:

Explanation:

Reference:

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

QUESTION 50

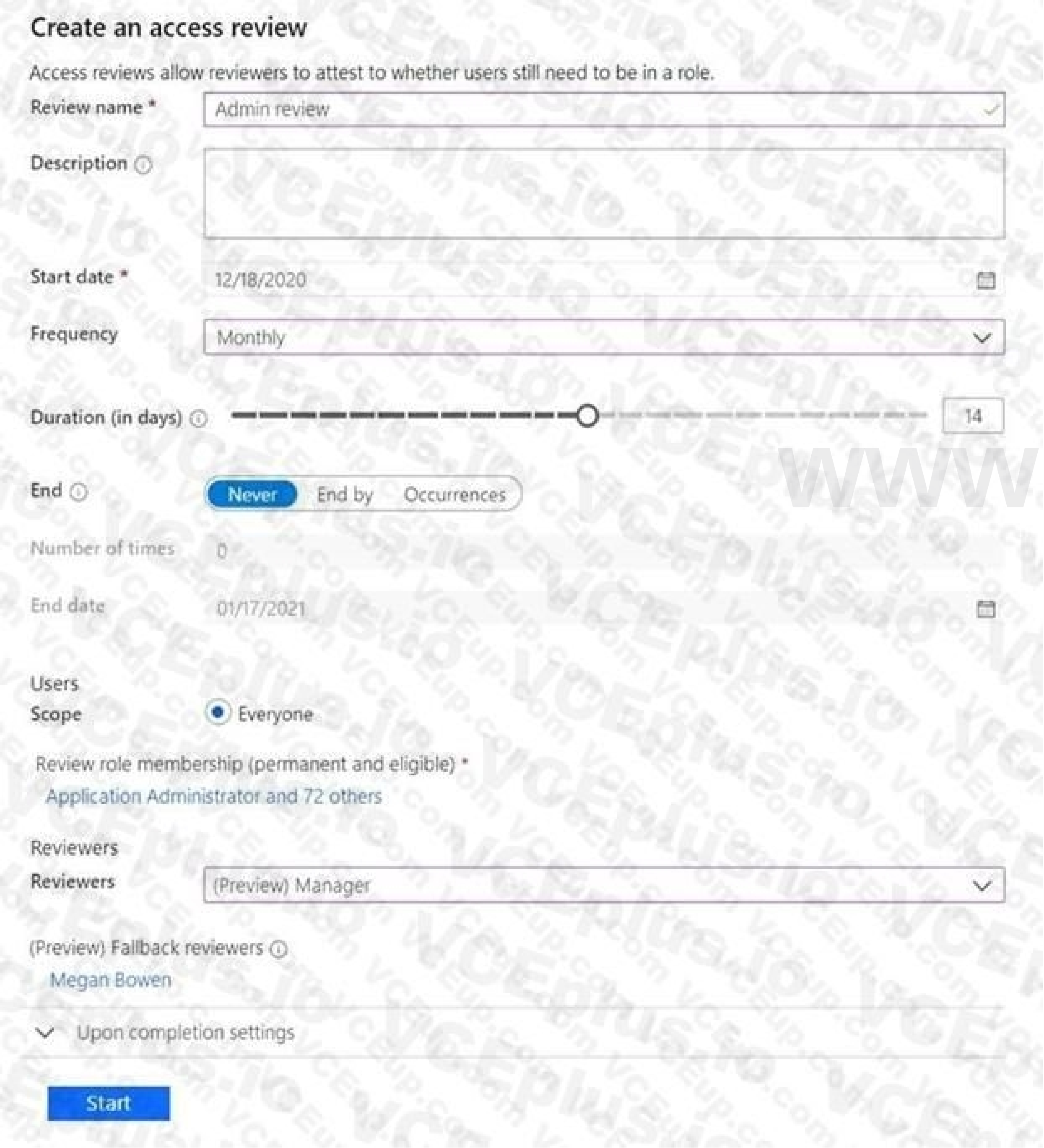
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

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

You need to ensure that the manager of each department receives the access reviews of their respective department.

Solution: You set Reviewers to Member (self).

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section:

QUESTION 51
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains an Azure AD enterprise application named App1.
A contractor uses the credentials of user1@outlook.com.
You need to ensure that you can provide the contractor with access to App1. The contractor must be able to authenticate as user1@outlook.com.
What should you do?

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

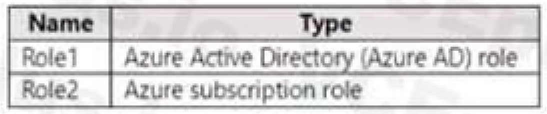
Correct Answer: D
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-addguest-usersportal

QUESTION 52
You have a Microsoft 365 subscription that contains the following:
• An Azure Active Directory (Azure AD) tenant that has an Azure Active Directory Premium P2 license
• A Microsoft SharePoint Online site named Site1
• A Microsoft Teams team named Team1
You need to create an entitlement management workflow to manage Site1 and Team1. What should you do first?

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

Correct Answer: A
Section:

QUESTION 53
You have an Azure subscription that contains the custom roles shown in the following table.



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

You need to create a custom Azure subscription role named Role3 by using the Azure portal. Role3 will use the baseline permissions of an existing role. Which roles can you clone to create Role3?

A. Role2 only
B. built-in Azure subscription roles only

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

Correct Answer: C
Section:

QUESTION 54
You have a Microsoft 365 tenant.
You have an Active Directory domain that syncs to the Azure Active Directory {Azure AD) tenant.
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. Cloud App Discovery in Microsoft Defender for Cloud Apps
B. enterprise applications in Azure AD
C. access reviews in Azure AD
D. Application Insights in Azure Monitor

Correct Answer: A
Section:

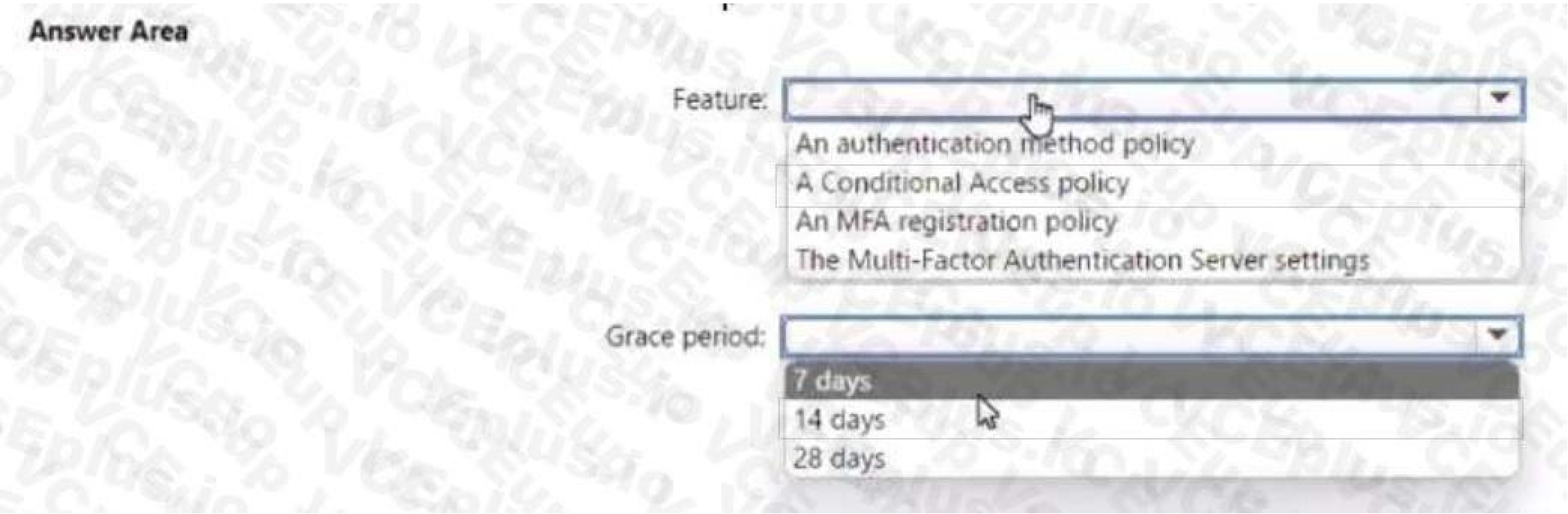
QUESTION 55
You have an Azure Active Directory (Azure AD) tenant that contains a user named User1.
You need to ensure that User1 can create new catalogs and add resources to the catalogs they own.
What should you do?

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

Correct Answer: B
Section:

QUESTION 56
HOTSPOT
You need to support the planned changes and meet the technical requirements for MFA.
Which feature should you use, and how long before the users must complete the registration? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

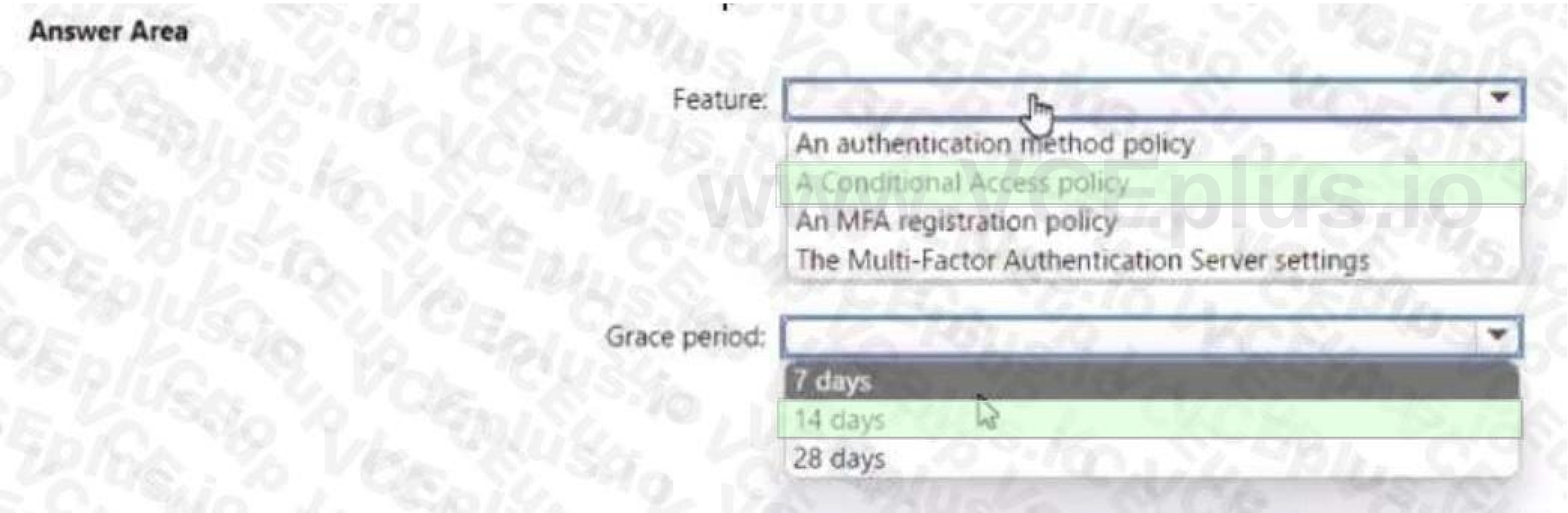
Feature:

- An authentication method policy
- A Conditional Access policy
- An MFA registration policy
- The Multi-Factor Authentication Server settings

Grace period:

- 7 days
- 14 days
- 28 days

Answer Area:



Answer Area

Feature:

- An authentication method policy
- [✓ A Conditional Access policy]
- An MFA registration policy
- The Multi-Factor Authentication Server settings

Grace period:

- 7 days
- [✓ 14 days]
- 28 days

Section:
Explanation:

QUESTION 57
You need to resolve the issue of the guest user invitations. What should you do for the Azure AD tenant?

A. Configure the Continuous access evaluation settings
B. Modify the External collaboration settings.
C. Configure the Access reviews settings
D. Configure a Conditional Access policy.

Correct Answer: B
Section:

QUESTION 58

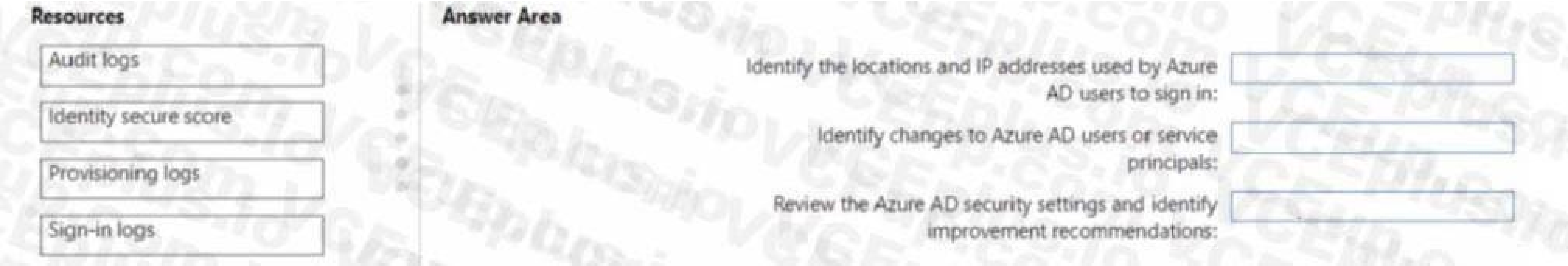
DRAG DROP

You have a Microsoft 365 E5 subscription. You need to perform the following tasks:

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

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

Select and Place:



Resources

- Audit logs
- Identity secure score
- Provisioning logs
- Sign-in logs

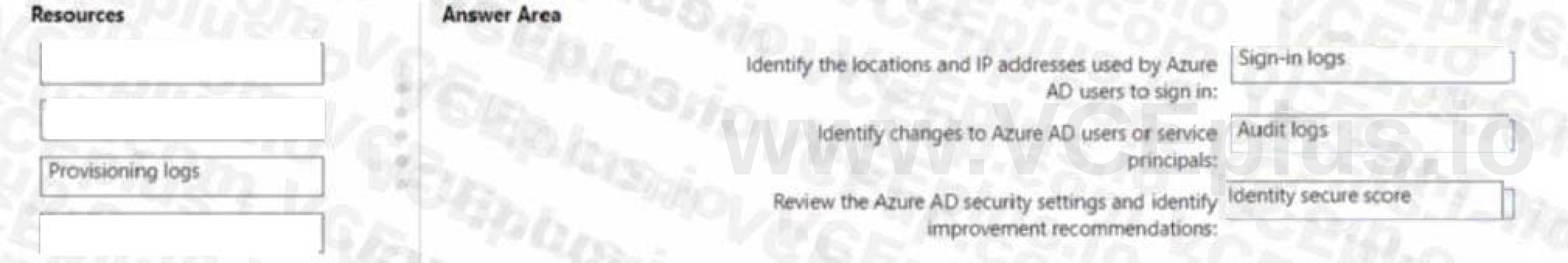
Answer Area

Identify the locations and IP addresses used by Azure AD users to sign in:

Identify changes to Azure AD users or service principals:

Review the Azure AD security settings and identify improvement recommendations:

Correct Answer:



Resources

- Provisioning logs

Answer Area

Identify the locations and IP addresses used by Azure AD users to sign in:	Sign-in logs
Identify changes to Azure AD users or service principals:	Audit logs
Review the Azure AD security settings and identify improvement recommendations:	Identity secure score

Section:

Explanation:

QUESTION 59

You have an Azure AD tenant that contains two users named User1 and User2. You plan to perform the following actions:

- Create a group named Group 1.
- Add User1 and User 2 to Group1.
- Assign Azure AD roles to Group1.

You need to create Group1.

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

NOTE: Each correct selection is worth one point

A. Group type: Microsoft 365 Membership type: Dynamic User

B. Group type: Security Membership type: Dynamic Device

C. Group type Security Membership type: Dynamic User

D. Group type Security Membership type: Assigned

E. Group type: Microsoft 365 Membership type: Assigned

Correct Answer: D, E

Section:

QUESTION 60

DRAG DROP

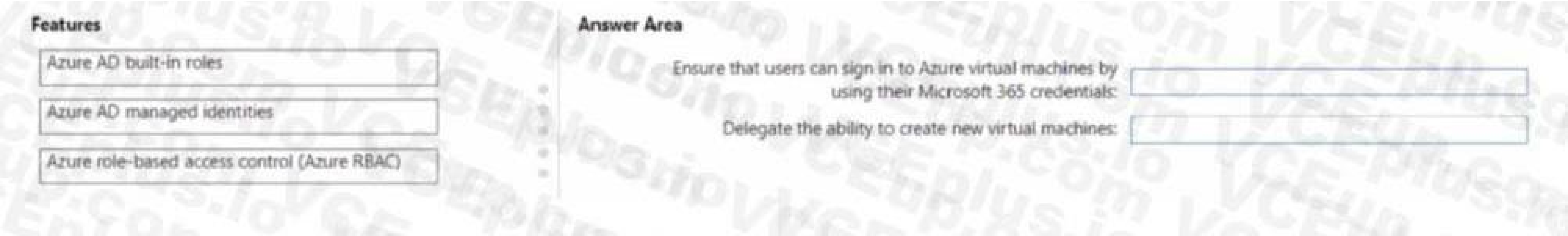
You have a Microsoft 365 E5 subscription and an Azure subscription. You need to meet the following requirements:

• Ensure that users can sign in to Azure virtual machines by using their Microsoft 365 credentials.

• Delegate the ability to create new virtual machines.

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

Select and Place:



Features

Azure AD built-in roles

Azure AD managed identities

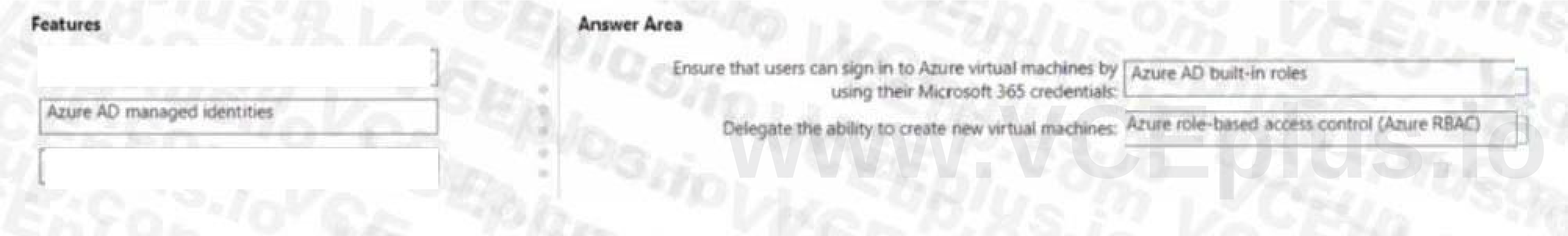
Azure role-based access control (Azure RBAC)

Answer Area

Ensure that users can sign in to Azure virtual machines by using their Microsoft 365 credentials:

Delegate the ability to create new virtual machines:

Correct Answer:



Features

Azure AD managed identities

Answer Area

Ensure that users can sign in to Azure virtual machines by using their Microsoft 365 credentials: Azure AD built-in roles

Delegate the ability to create new virtual machines: Azure role-based access control (Azure RBAC)

Section:

Explanation:

QUESTION 61

You have a Microsoft 365 ES subscription that contains a user named User1. User1 is eligible for the Application administrator role.

User1 needs to configure a new connector group for an application proxy.

What should you to activate the role for User1?

A. the Microsoft Defender for Cloud Apps portal

B. the Microsoft 365 admin center

C. the Azure Active Directory admin center

D. the Microsoft 365 Defender portal

Correct Answer: C

Section:

QUESTION 62

You have a Microsoft 365 ES subscription that user Microsoft Defender for Cloud Apps and Yammer.

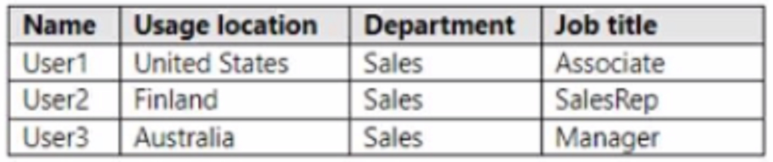
You need prevent users from signing in to Yammer from high-risk locations.

What should you do in the Microsoft Defender for Cloud Apps portal?

A. Create an access Policy.
B. Create an activity policy.
C. Unsanction Yammer.
D. Create an anomaly detection policy.

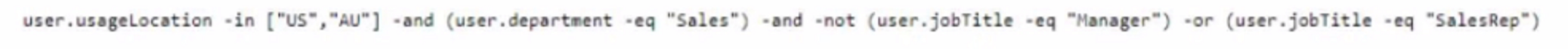
Correct Answer: A
Section:

QUESTION 63
You have an Azure Ad tenant that contains the users show in the following table.



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

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



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

Which users will be added to the group?

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

Correct Answer: D
Section:

QUESTION 64
You have an Azure subscription that uses Azure AD Privileged Identity Management (PIM).
You need to identify users that are eligible for the Cloud Application Administrator role.
Which blade in the Privileged Identity Management settings should you use?

A. Azure resources
B. Privileged access groups
C. Review access
D. Azure AD roles

Correct Answer: D
Section:

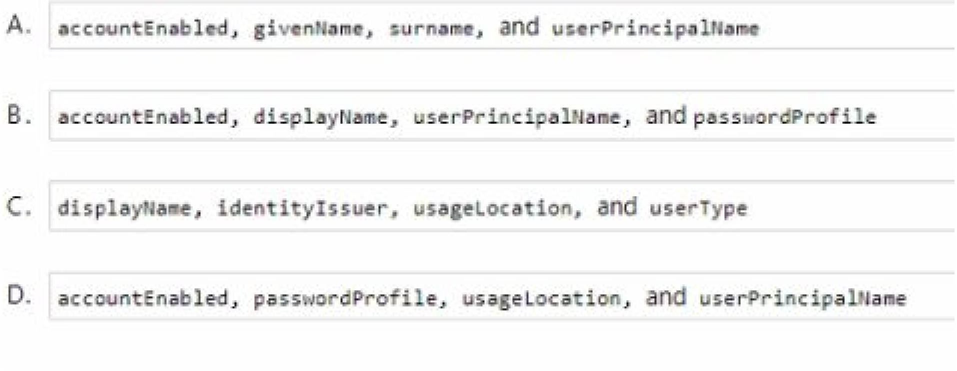
QUESTION 65
You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1. You need to be notified if a user downloads more than 50 files in one minute from Site1.
Which type of policy should you create in the Microsoft Defender for Cloud Apps portal?

A. session policy

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

Correct Answer: C
Section:

QUESTION 66
You have an Azure AD tenant.
You need to bulk create 25 new user accounts by uploading a template file.
Which properties are required in the template file?



A. accountEnabled, givenName, surname, and userPrincipalName

B. accountEnabled, displayName, userPrincipalName, and passwordProfile

C. displayName, identityIssuer, usageLocation, and userType

D. accountEnabled, passwordProfile, usageLocation, and userPrincipalName

A. Option A
B. Option B
C. Option C
D. Option D

Correct Answer: B
Section:

QUESTION 67
You have a Microsoft 365 E5 subscription.
Users authorize third-party cloud apps to access their data.
You need to configure an alert that will be triggered when an app requires high permissions and is authorized by more than 20 users.
Which type of policy should you create in the Microsoft Defender for Cloud Apps portal?

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

Correct Answer: C
Section:

QUESTION 68
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it as a result these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription.

You create a user named User1.
You need to ensure that User1 can update the status of identity Secure Score improvement actions.
Solution: You assign the SharePoint Administrator role to User1
Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section:

QUESTION 69
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 ES subscription.
You create a user named User1.
You need to ensure that User1 can update the status of identity Secure Score improvement actions.
Solution: You assign the Exchange Administrator role to User1.

A. Yes
B. No

Correct Answer: B
Section:

QUESTION 70
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it as a result these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription.
You create a user named User1.
You need to ensure that User1 can update the status of identity Secure Score improvement actions.
Solution: You assign the User Administrator role to User1.
Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section:

QUESTION 71
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 ES subscription.
You create a user namedUser1.
You need to ensure that User1 can update the status of identity Secure Score improvement actions.

Solution: You assign the Security Operator role User1.
Does this meet the goal?

A. Yes
B. No

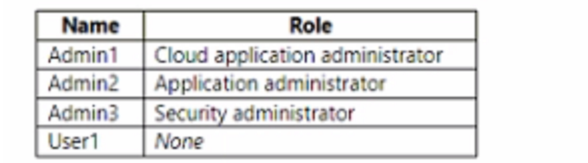
Correct Answer: B
Section:

QUESTION 72
You have an Azure AD tenant
You configure User consent settings to allow users to provide consent to apps from verified publishers.
You need to ensure that the users can only provide consent to apps that require low impact permissions.
What should you do?

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

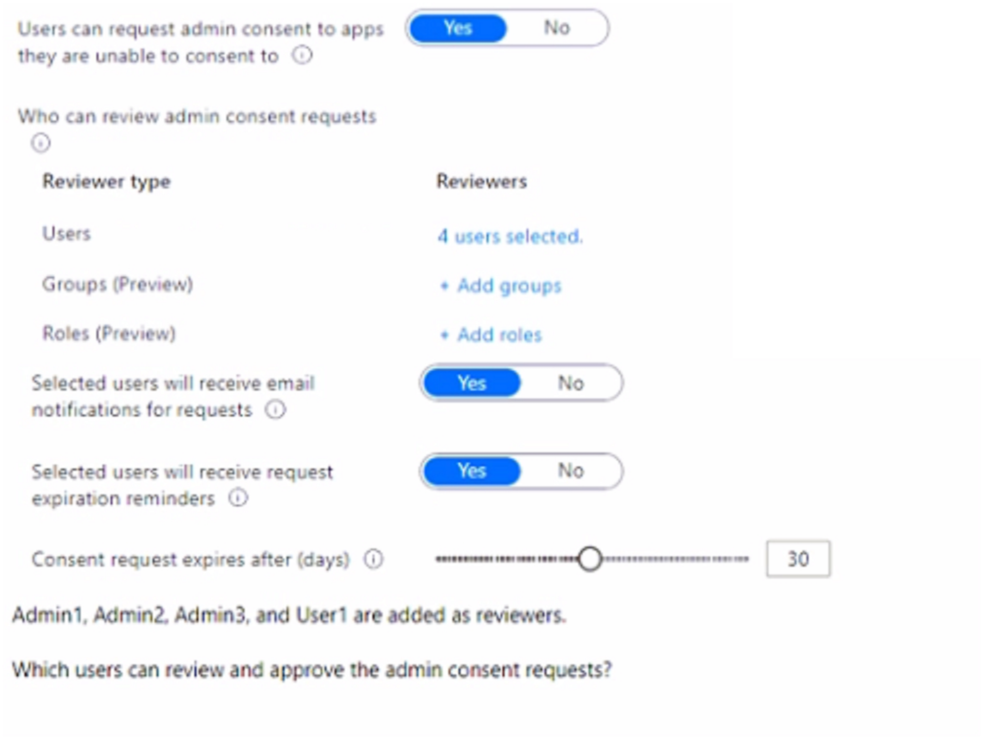
Correct Answer: B
Section:

QUESTION 73
You have an Azure AD tenant that contains the users shown in the following table.



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

You add an enterprise application named App1 to Azure AD and set User1 as the owner of App1 requires admin consent to access Azure AD before the app can be used.
You configure the Admin consent requests strong as shown in the following exhibit.
Admin consent requests.



Users can request admin consent to apps they are unable to consent to ⓘ: ● Yes ○ No

Who can review admin consent requests ⓘ

Reviewer type	Reviewers
Users	4 users selected.
Groups (Preview)	+ Add groups
Roles (Preview)	+ Add roles

Selected users will receive email notifications for requests ⓘ: ● Yes ○ No

Selected users will receive request expiration reminders ⓘ: ● Yes ○ No

Consent request expires after (days) ⓘ: 30

Admin1, Admin2, Admin3, and User1 are added as reviewers.

Which users can review and approve the admin consent requests?

A. Admm1 only
B. Admm1 and Admin2 only
C. Admm1 Admm2 and Admin3 only
D. Admln1, Admin2. and User1 only
E. Admm1 Admm2. Admm3, and User1

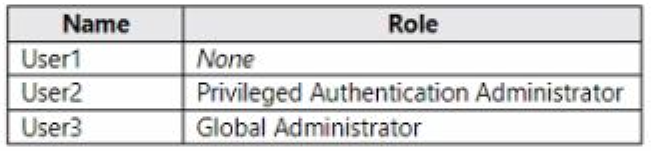
Correct Answer: B
Section:

QUESTION 74
You have a Microsoft 365 subscription that contains a user named User1.
You need to ensure that User1 can create access reviews for Azure AD roles. The solution must use the principal of least privilege.
Which role should you assign to User1?

A. Privileged role administrator
B. Identify Governance administrator
C. User administrator
D. User Access Administrate

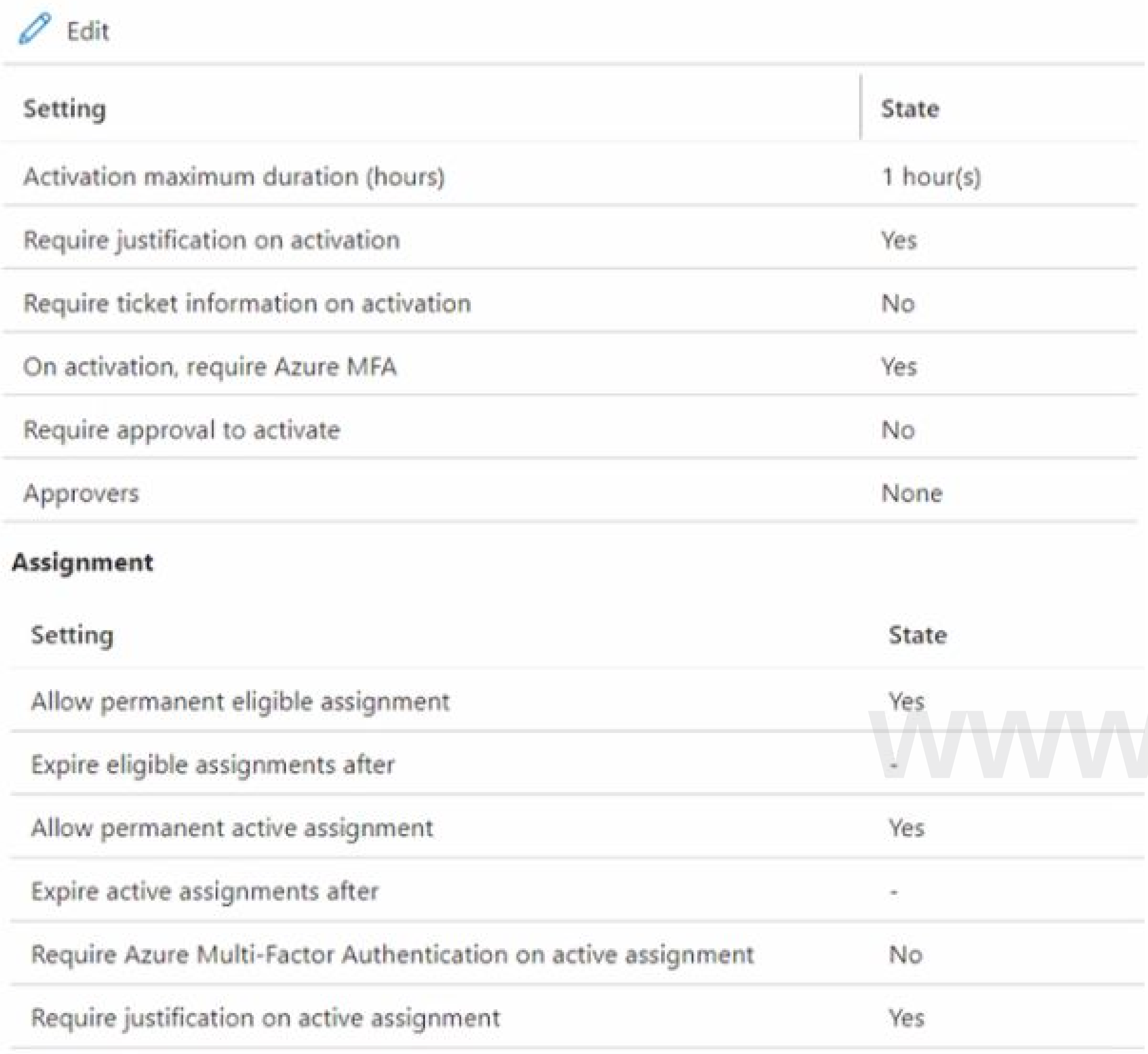
Correct Answer: B
Section:

QUESTION 75
HOTSPOT
You have an Azure AD tenant contains the users shown in the following table.



Name	Role
User1	*None*
User2	Privileged Authentication Administrator
User3	Global Administrator

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



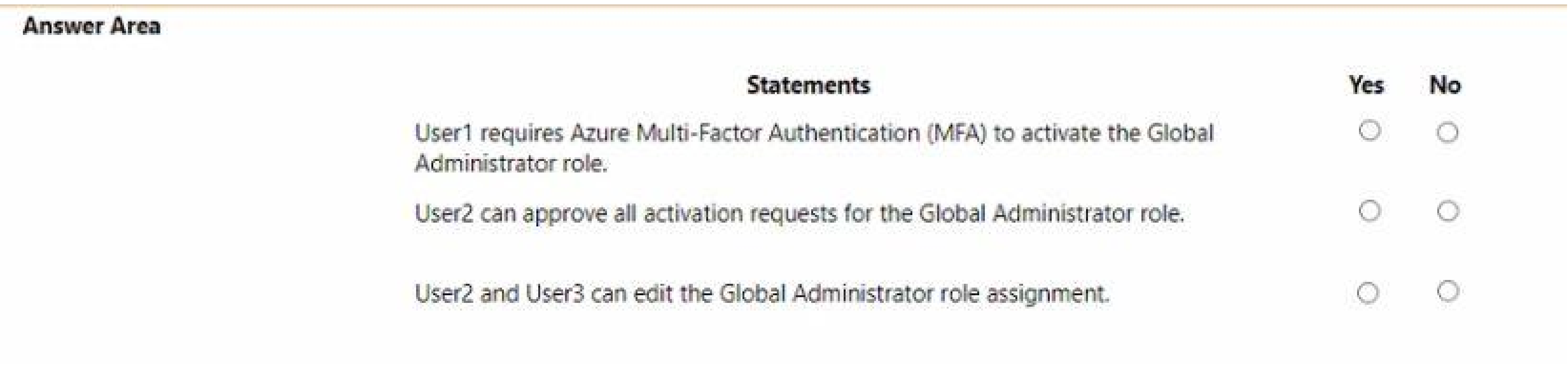
Setting	State
Activation maximum duration (hours)	1 hour(s)
Require justification on activation	Yes
Require ticket information on activation	No
On activation, require Azure MFA	Yes
Require approval to activate	No
Approvers	None

Assignment

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

User 1 is eligible for the Global Administrator role.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

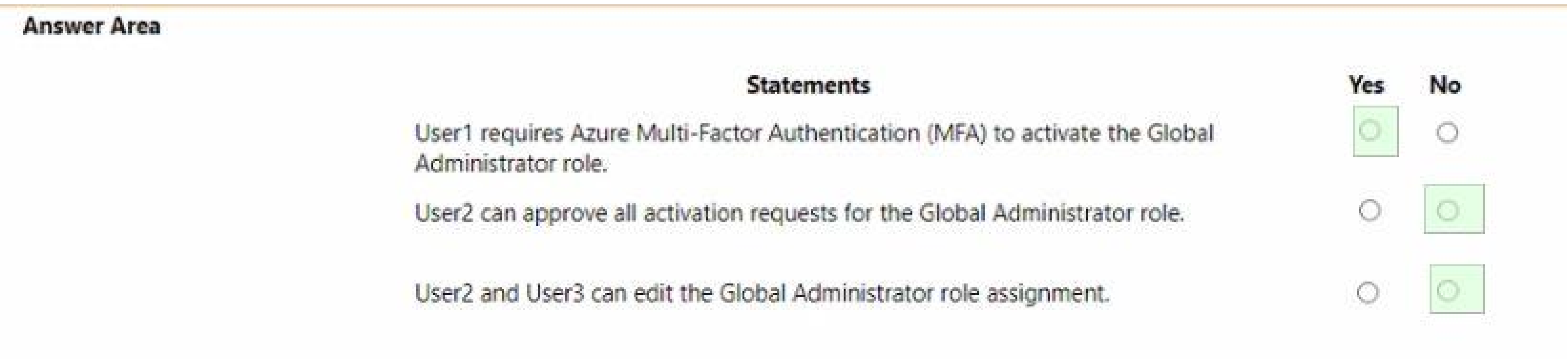
Hot Area:



Answer Area

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

Answer Area:



Answer Area

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

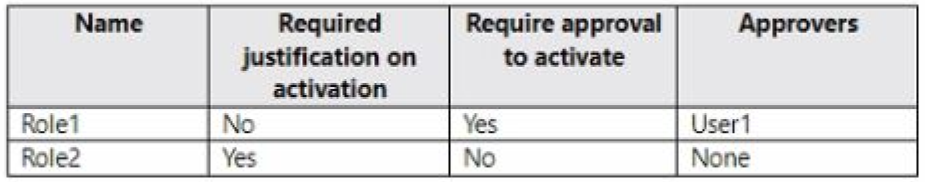
Section:
Explanation:

QUESTION 76

HOTSPOT

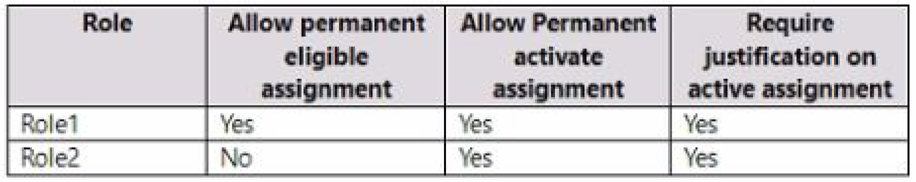
You have a Microsoft 365 E5 subscription that contains three users named User1, User2, and User3.

You have two Azure AD roles that have the Activation settings shown in the following table.



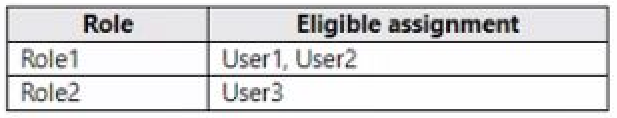
Name	Required justification on activation	Require approval to activate	Approvers
Role1	No	Yes	User1
Role2	Yes	No	None

The Azure AD roles have the Assignment settings shown in the following table.



Role	Allow permanent eligible assignment	Allow Permanent activate assignment	Require justification on active assignment
Role1	Yes	Yes	Yes
Role2	No	Yes	Yes

The Azure AD roles have the eligible users shown in the following table.

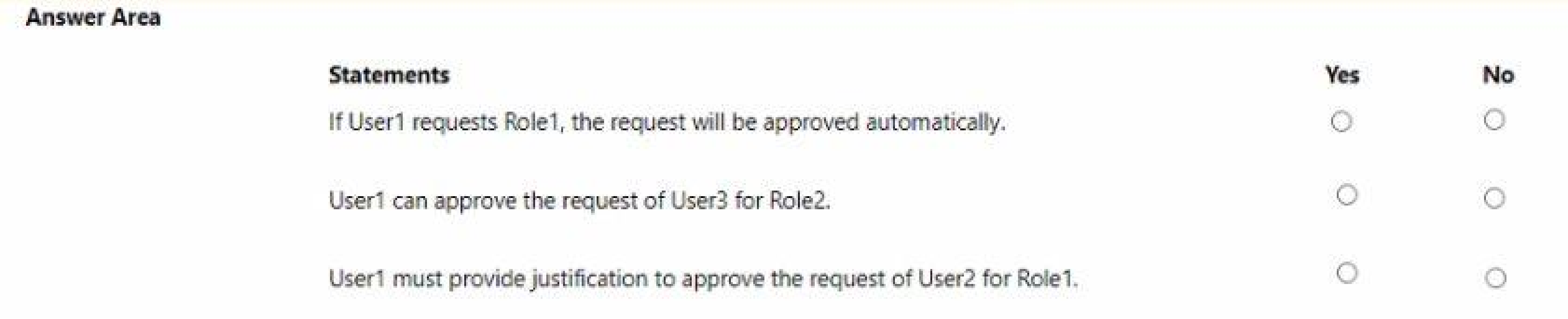


Role	Eligible assignment
Role1	User1, User2
Role2	User3

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

NOTE: Each correct selection is worth one point.

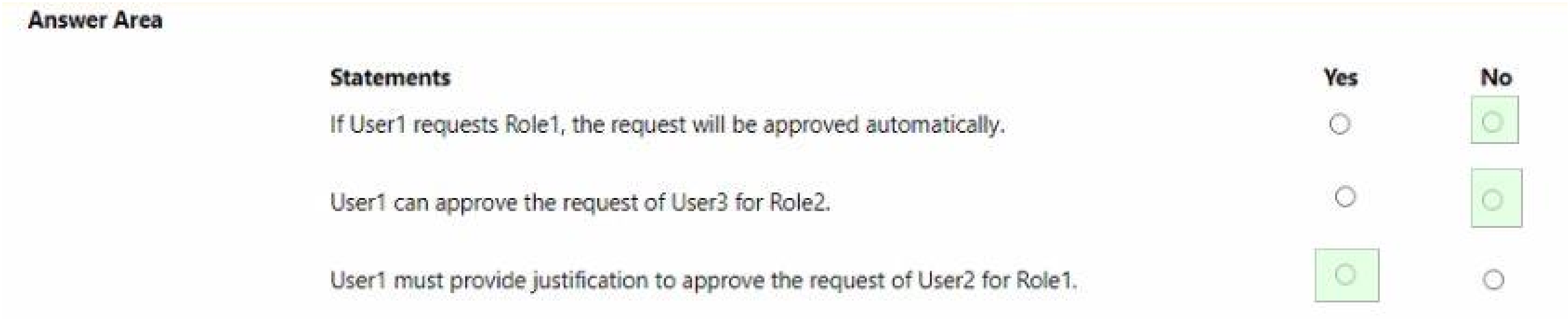
Hot Area:



Answer Area

Statements	Yes	No
If User1 requests Role1, the request will be approved automatically.	○	○
User1 can approve the request of User3 for Role2.	○	○
User1 must provide justification to approve the request of User2 for Role1.	○	○

Answer Area:



Answer Area

Statements	Yes	No
If User1 requests Role1, the request will be approved automatically.	○	[✓ ○]
User1 can approve the request of User3 for Role2.	○	[✓ ○]
User1 must provide justification to approve the request of User2 for Role1.	[✓ ○]	○

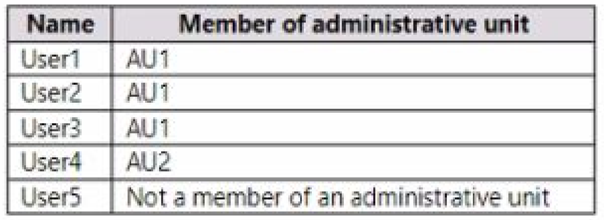
Section:
Explanation:

QUESTION 77
A user named User1 receives an error message when attempting to access the Microsoft Defender for Cloud Apps portal.
You need to identify the cause of the error. The solution must minimize administrative effort.
What should you use?

A. Log Analytics
B. sign-in logs
C. audit logs
D. provisioning logs

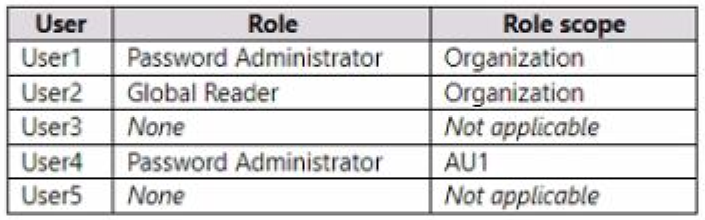
Correct Answer: B
Section:

QUESTION 78
HOTSPOT
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.



Name	Member of administrative unit
User1	AU1
User2	AU1
User3	AU1
User4	AU2
User5	Not a member of an administrative unit

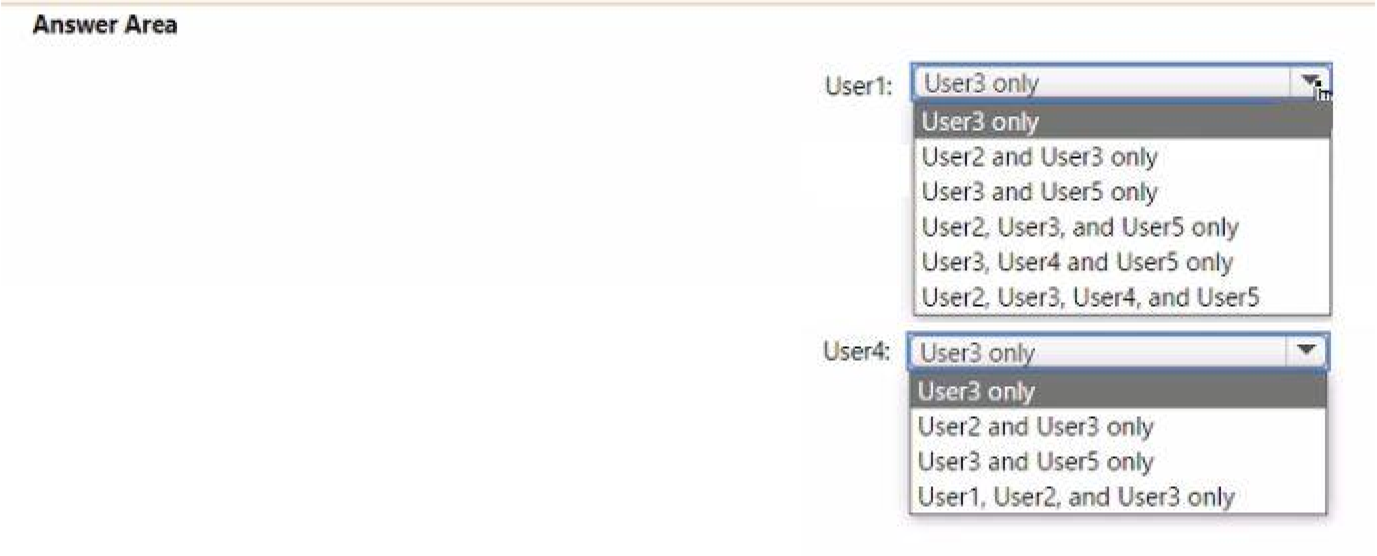
The users are assigned the roles shown in the following table.



User	Role	Role scope
User1	Password Administrator	Organization
User2	Global Reader	Organization
User3	*None*	*Not applicable*
User4	Password Administrator	AU1
User5	*None*	*Not applicable*

For which users can User1 and User4 reset passwords? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

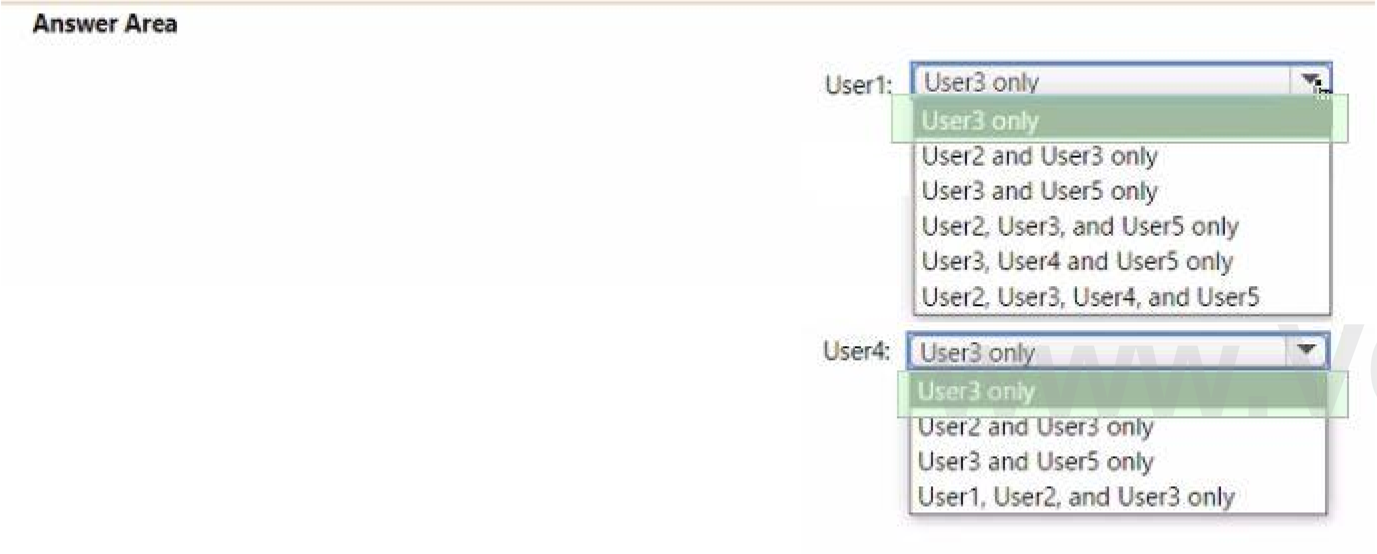
User1: User3 only

User3 only
User2 and User3 only
User3 and User5 only
User2, User3, and User5 only
User3, User4 and User5 only
User2, User3, User4, and User5

User4: User3 only

User3 only
User2 and User3 only
User3 and User5 only
User1, User2, and User3 only

Answer Area:



Answer Area

User1: User3 only

User3 only
User2 and User3 only
User3 and User5 only
User2, User3, and User5 only
User3, User4 and User5 only
User2, User3, User4, and User5

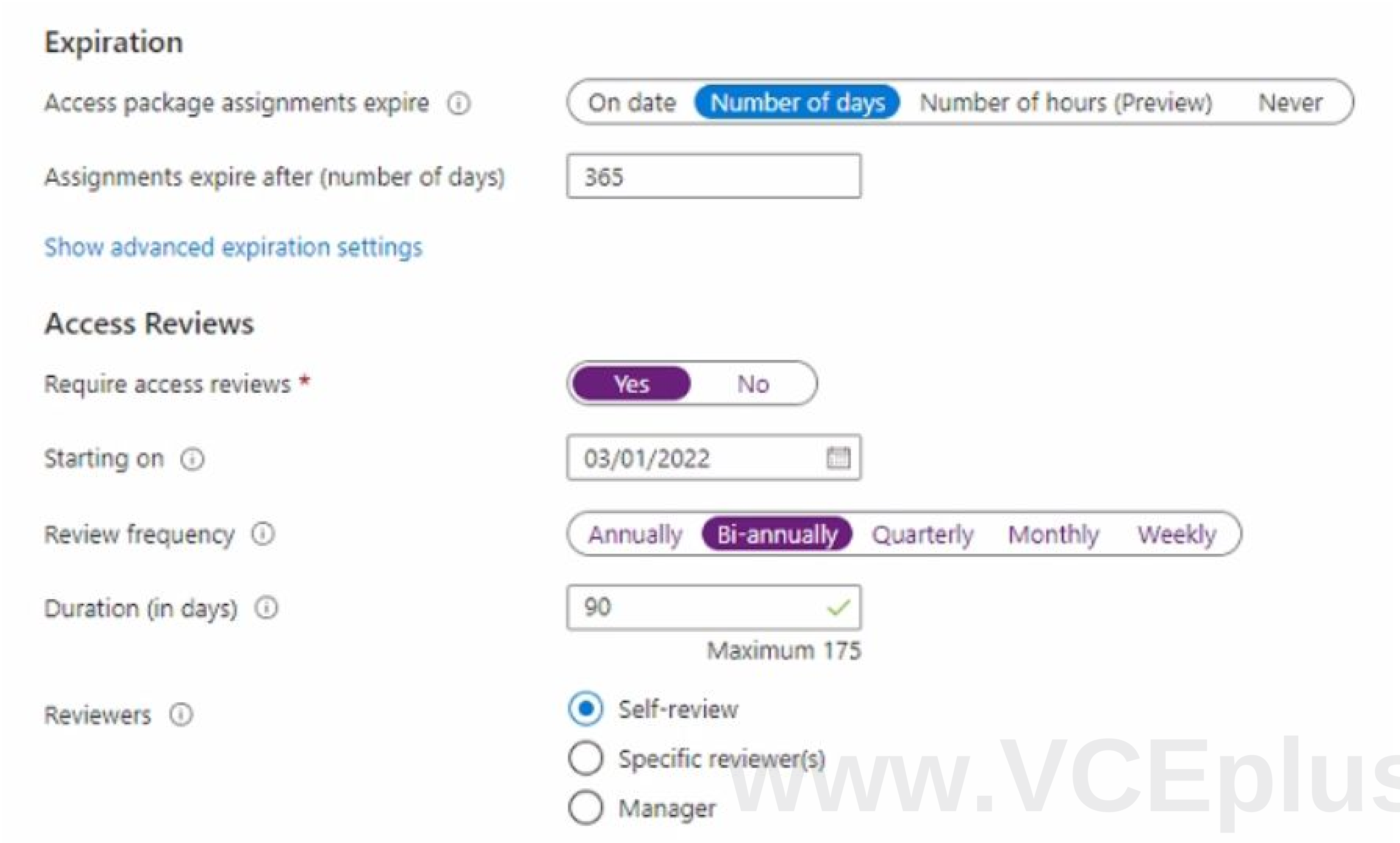
User4: User3 only

User3 only
User2 and User3 only
User3 and User5 only
User1, User2, and User3 only

Section:
Explanation:

QUESTION 79

You have an Azure AD tenant that contains an access package named Package1 and a user named User1. Package1 is configured as shown in the following exhibit.



Expiration

Access package assignments expire: On date [✓ Number of days] Number of hours (Preview) Never

Assignments expire after (number of days): 365

Show advanced expiration settings

Access Reviews

Require access reviews *: [✓ Yes] No

Starting on: 03/01/2022

Review frequency: Annually [✓ Bi-annually] Quarterly Monthly Weekly

Duration (in days): 90 ✓

Maximum 175

Reviewers:
● Self-review
○ Specific reviewer(s)
○ Manager

You need to ensure that User1 can modify the review frequency of Package1. The solution must use the principle of least privilege.
Which role should you assign to User1?

A. Privileged role administrator
B. User administrator
C. External Identity Provider administrator
D. Security administrator

Correct Answer: A
Section:

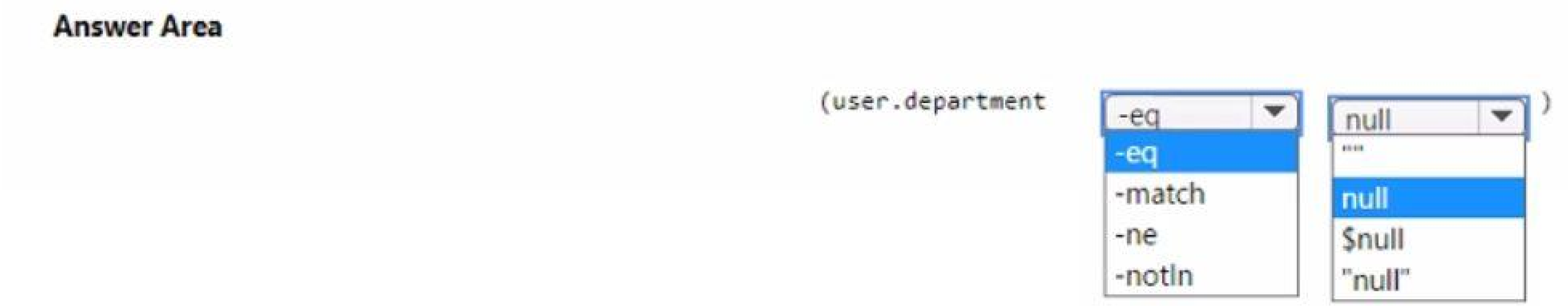
QUESTION 80
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps.
You need to identify which users access Facebook from their devices and browsers. The solution must minimize administrative effort.
What should you do first?

A. From the Microsoft Defender for Cloud Apps portal, unsanctioned Facebook.
B. Create an app configuration policy in Microsoft Endpoint Manager.
C. Create a Defender for Cloud Apps access policy.
D. Create a Conditional Access policy.

Correct Answer: C
Section:

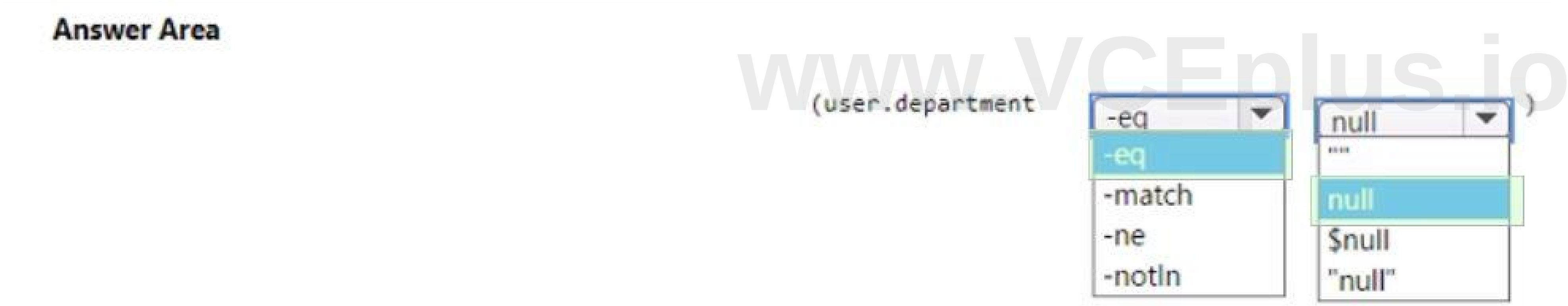
QUESTION 81
HOTSPOT
You have a Microsoft 365 E5 subscription.
You need to create a dynamic user group that will include all the users that do NOT have a department defined in their user profile.
How should you complete the membership rule? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:


Answer Area

(user.department -eq null)

Answer Area:


Answer Area

(user.department -eq null)

Section:
Explanation: