Microsoft.SC-300.vMay-2024.by.HerryQuan.119q

Number: SC-300
Passing Score: 800
Time Limit: 120
File Version: 23.0

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

Case Study

Contoso, Ltd

Overview

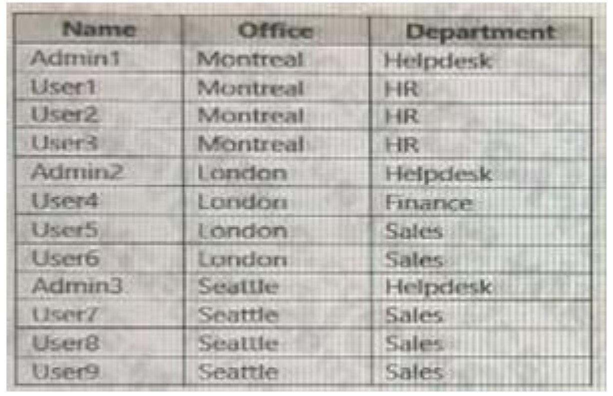
Contoso, Ltd is a consulting company that has a main office in Montreal offices in London and Seattle.

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

Existing Environment

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

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



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

Microsoft 365/Azure Environment

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

Microsoft Office 365 Enterprise E5

Enterprise Mobility + Security

Windows 10 Enterprise E5

Project Plan 3

Azure AD Connect is configured between azure AD and Active Directory Domain Serverless (AD DS).

Only the Contoso Resources OU is synced.

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

User administrators currently use the Microsoft 365 admin center to manually assign licenses, All user have all licenses assigned besides following exception:

The users in the London office have the Microsoft 365 admin center to manually assign licenses. All user have licenses assigned besides the following exceptions:

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

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

Security defaults are disabled for Contoso.com.

Contoso uses Azure AD Privileged identity Management (PIM) to project administrator roles.

Problem Statements

Contoso identifies the following issues:

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

Planned Changes

Contoso plans to implement the following changes.

Implement self-service password reset (SSPR). Analyze Azure audit activity logs by using Azure Monitor-Simplify license allocation for new users added to the tenant. Collaborate with the users at Fabrikam on a joint marketing campaign.

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

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

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

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

Technical Requirements

Contoso identifies the following technical requirements:

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

QUESTION 1
You create a Log Analytics workspace.
You need to implement the technical requirements for auditing.
What should you configure in Azure AD?

A. Company branding
B. Diagnostics settings
C. External Identities
D. App registrations

Correct Answer: B
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/overview-monitoring

QUESTION 2
You need to sync the ADatum users. The solution must meet the technical requirements.
What should you do?

A. From the Microsoft Azure Active Directory Connect wizard, select Customize synchronization options.
B. From PowerShell, run Set-ADSyncScheduler.
C. From PowerShell, run Start-ADSyncSyncCycle.
D. From the Microsoft Azure Active Directory Connect wizard, select Change user sign-in.

Correct Answer: A
Section:
Explanation:
You need to select Customize synchronization options to configure Azure AD Connect to sync the Adatum organizational unit (OU).

QUESTION 3
You need to meet the planned changes and technical requirements for App1.
What should you implement?

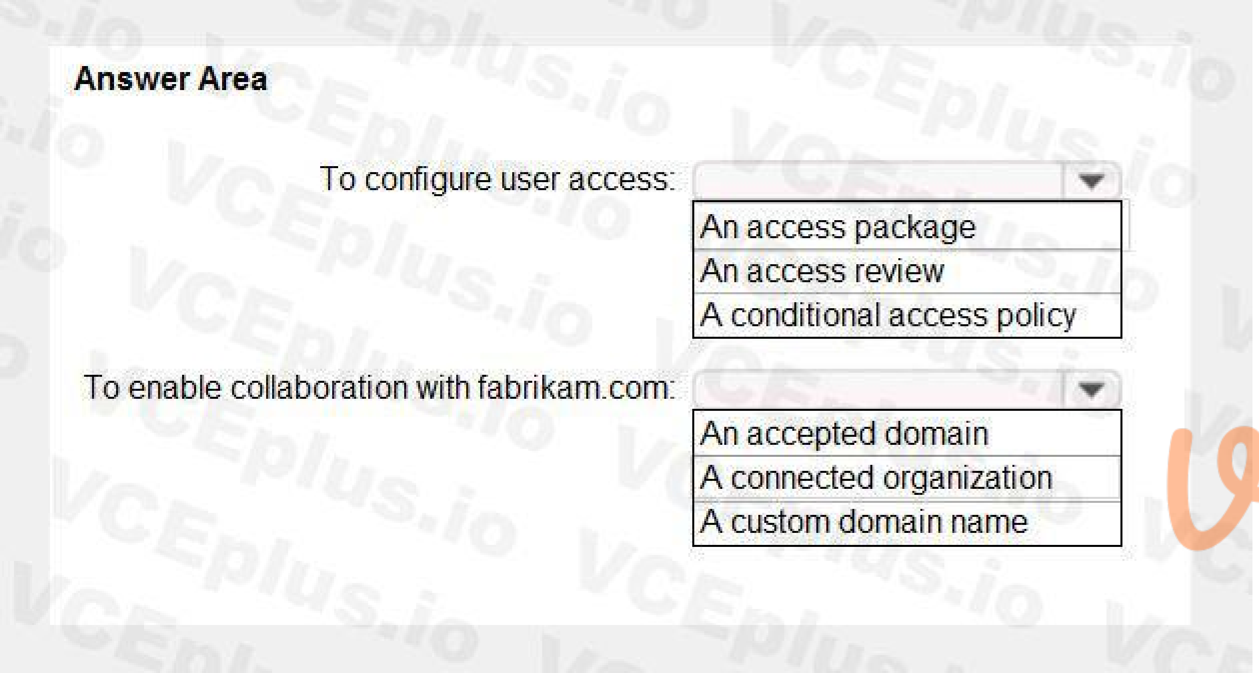
A. a policy set in Microsoft Endpoint Manager
B. an app configuration policy in Microsoft Endpoint Manager
C. an app registration in Azure AD
D. Azure AD Application Proxy

Correct Answer: C

Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app

QUESTION 4
HOTSPOT
You need to implement the planned changes and technical requirements for the marketing department.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:

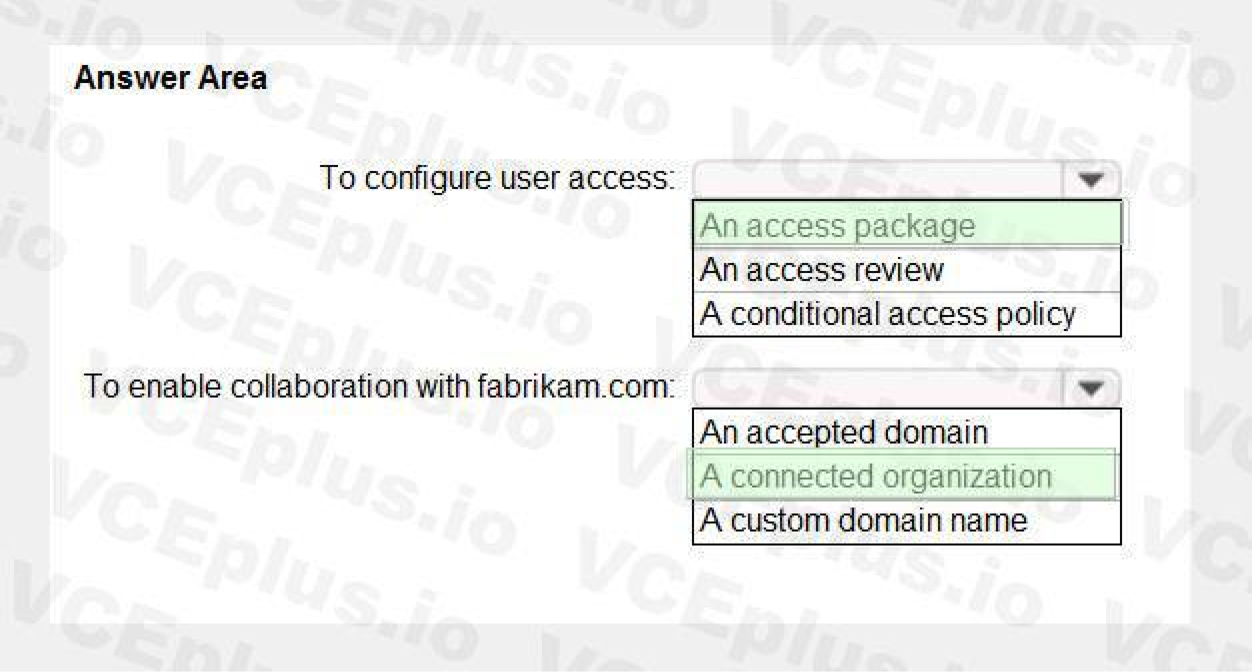


Answer Area

To configure user access:
- An access package
- An access review
- A conditional access policy

To enable collaboration with fabrikam.com:
- An accepted domain
- A connected organization
- A custom domain name

Answer Area:



Answer Area

To configure user access:
- [✓ An access package]
- An access review
- A conditional access policy

To enable collaboration with fabrikam.com:
- An accepted domain
- [✓ A connected organization]
- A custom domain name

Section:

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

QUESTION 5

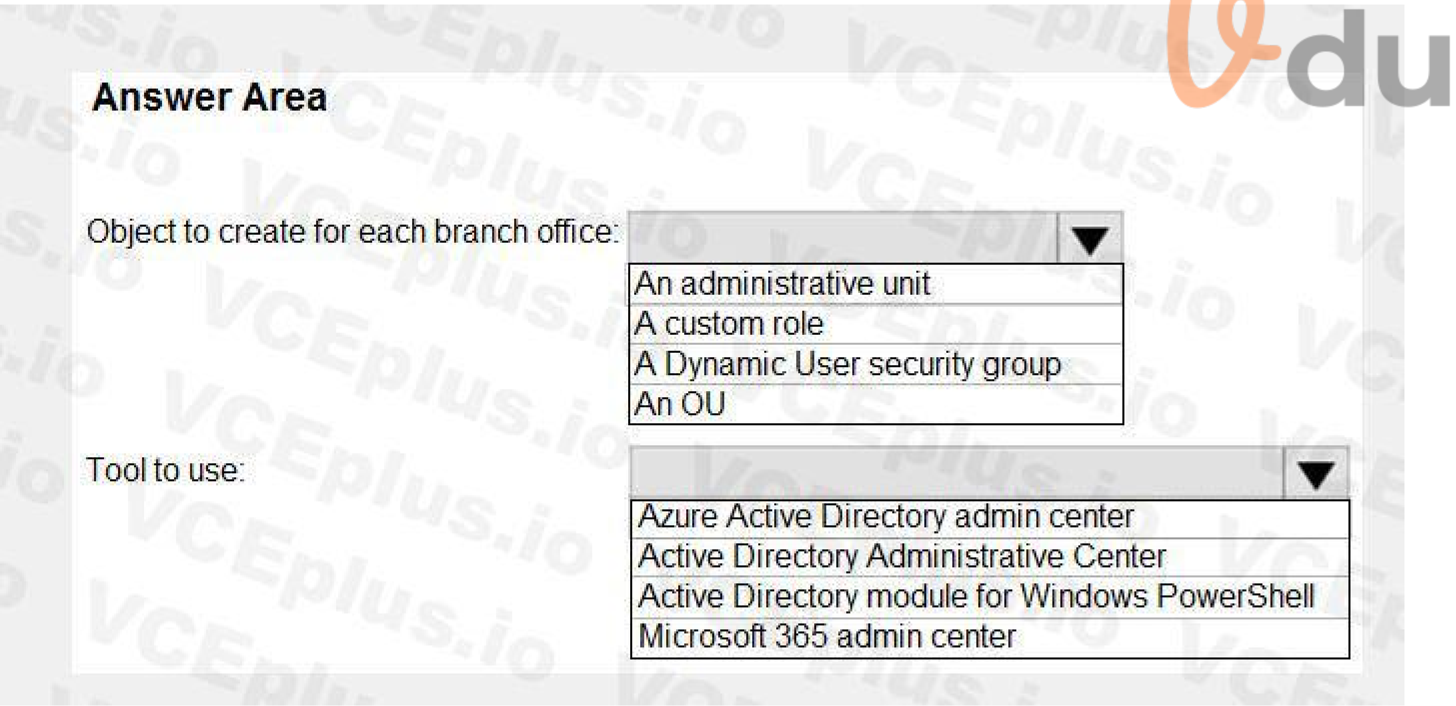
You need to allocate licenses to the new users from A. Datum. The solution must meet the technical requirements. Which type of object should you create?

A. a distribution group
B. a Dynamic User security group
C. an administrative unit
D. an OU

Correct Answer: C
Section:

QUESTION 6
HOTSPOT
You need to meet the technical requirements for license management by the helpdesk administrators.
What should you create first, and which tool should you use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:

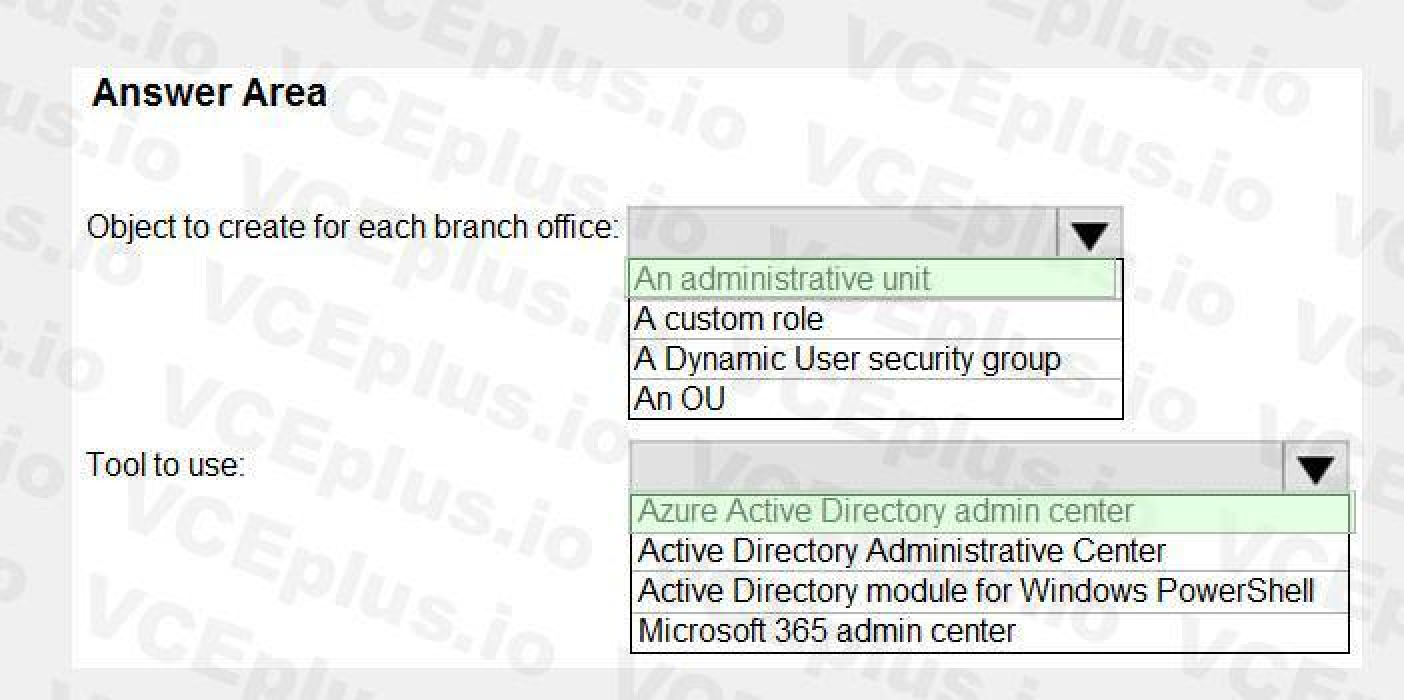


Answer Area

Object to create for each branch office: ▼
- An administrative unit
- A custom role
- A Dynamic User security group
- An OU

Tool to use: ▼
- Azure Active Directory admin center
- Active Directory Administrative Center
- Active Directory module for Windows PowerShell
- Microsoft 365 admin center

Answer Area:



Answer Area

Object to create for each branch office:

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

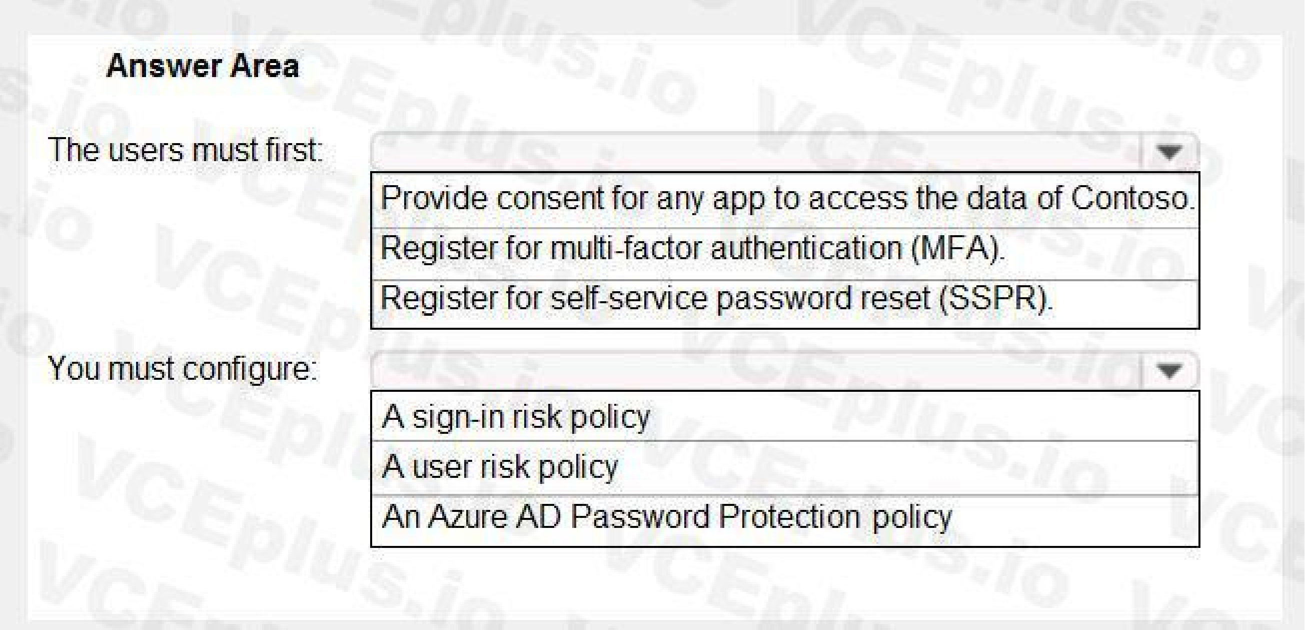
Tool to use:

- [✓ Azure Active Directory admin center]
- Active Directory Administrative Center
- Active Directory module for Windows PowerShell
- Microsoft 365 admin center

Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/roles/administrative-units
https://docs.microsoft.com/en-us/azure/active-directory/roles/admin-units-manage

QUESTION 7
HOTSPOT
You need to meet the technical requirements for the probability that user identities were compromised.
What should the users do first, and what should you configure? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

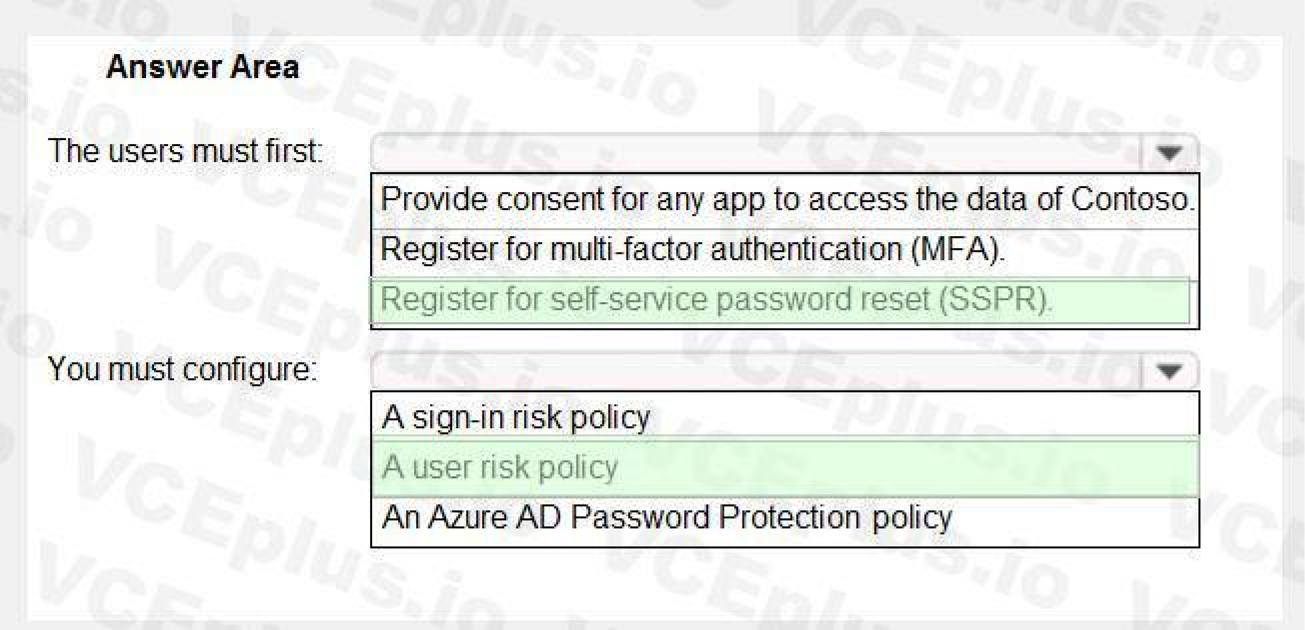
The users must first:

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

You must configure:

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

Answer Area:



Answer Area

The users must first:

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

You must configure:

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

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

QUESTION 8
You need to locate licenses to the ADatum users. The solution must need the technical requirements.
Which type of object should you create?

A. A Dynamo User security group
B. An OU
C. A distribution group
D. An administrative unit

Correct Answer: D
Section:

QUESTION 9
You need to meet the planned changes for the User administrator role.
What should you do?

A. Create an access review.
B. Modify Role settings
C. Create an administrator unit.
D. Modify Active Assignments.

Correct Answer: B
Section:
Explanation:
Role Setting details is where you need to be: Role setting details - User Administrator Privileged Identity Management | Azure AD roles Default Setting State Require justification on activation Yes Require ticket information on activation No
On activation, require Azure MFA Yes Require approval to activate No Approvers None

Case Study

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.

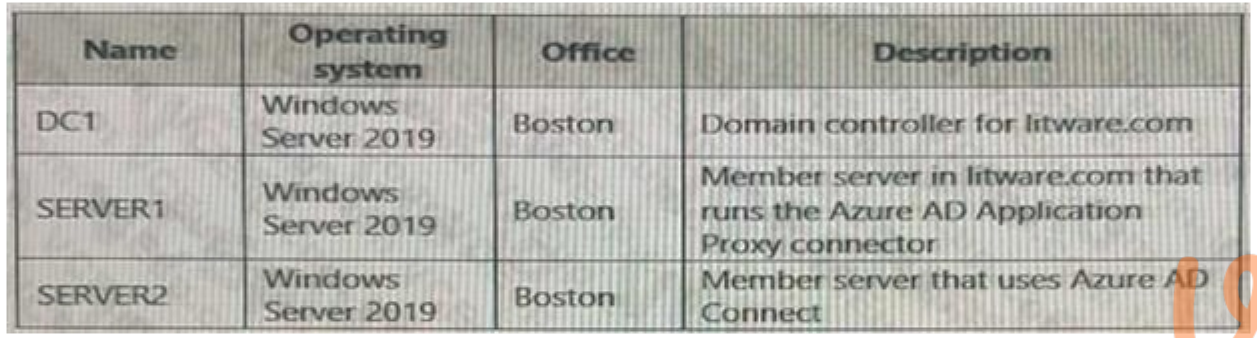
Cloud Environment

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.

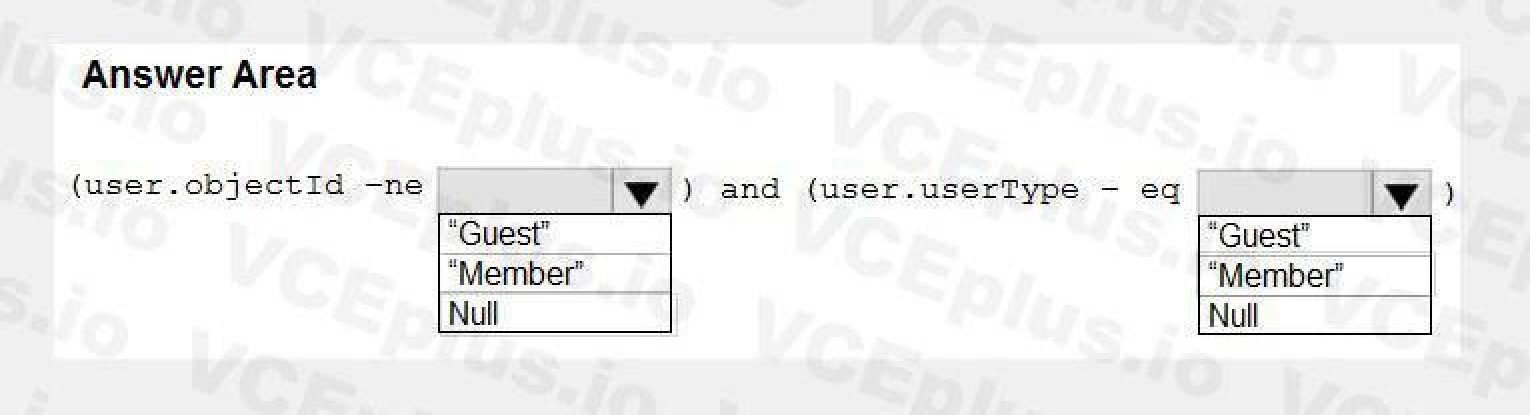
QUESTION 1

HOTSPOT

You need to 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.

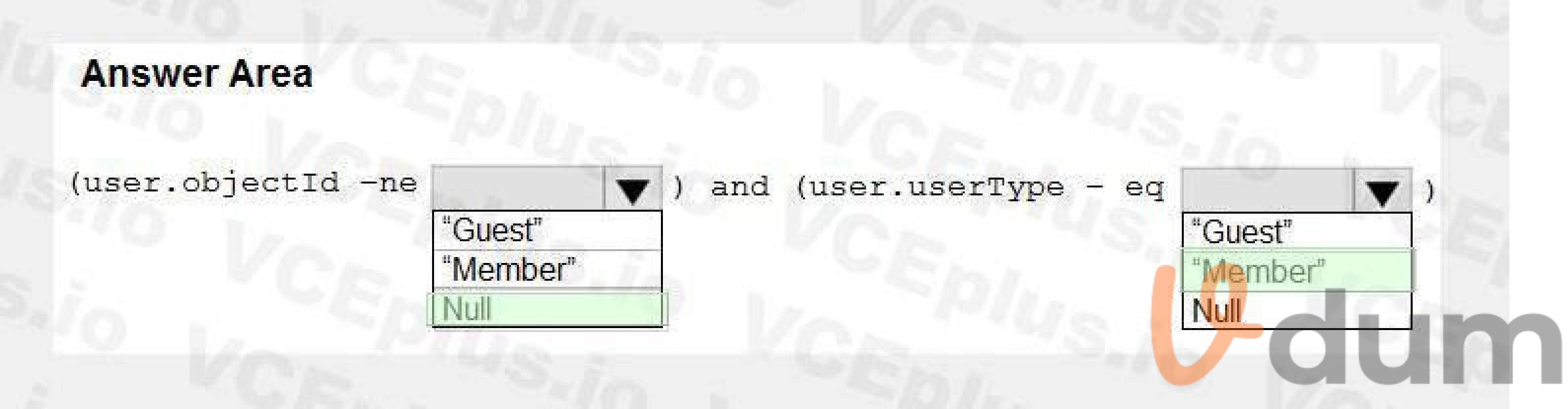
Hot Area:



Answer Area

(user.objectId -ne ["Guest" / "Member" / Null]) and (user.userType – eq ["Guest" / "Member" / Null])

Answer Area:



Answer Area

(user.objectId -ne ["Guest" / "Member" / [✓ Null]]) and (user.userType – eq ["Guest" / [✓ "Member"] / Null])

Section:
Explanation:

QUESTION 2
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 3
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:

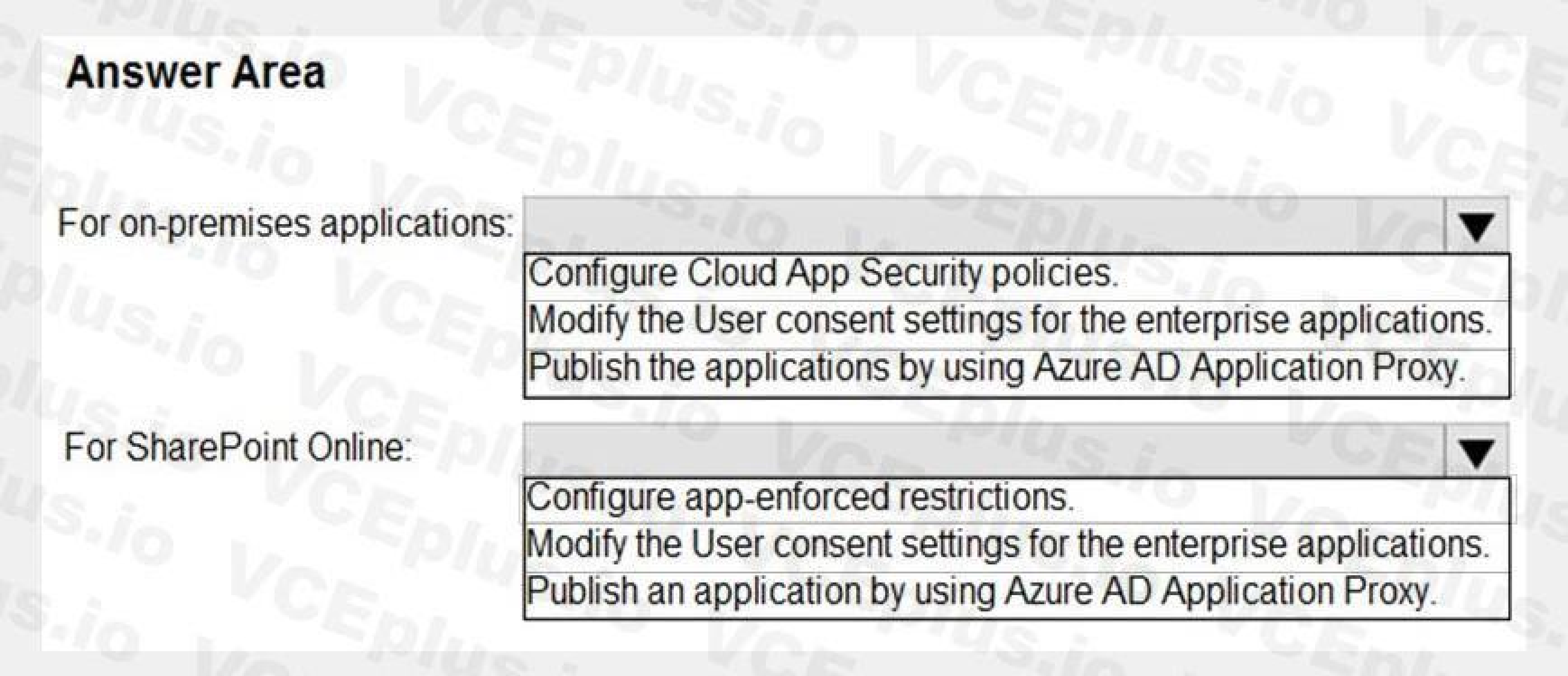
QUESTION 4
You need to track application access assignments by using Identity Governance. The solution must meet the delegation requirements.
What should you do first?

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 5
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:

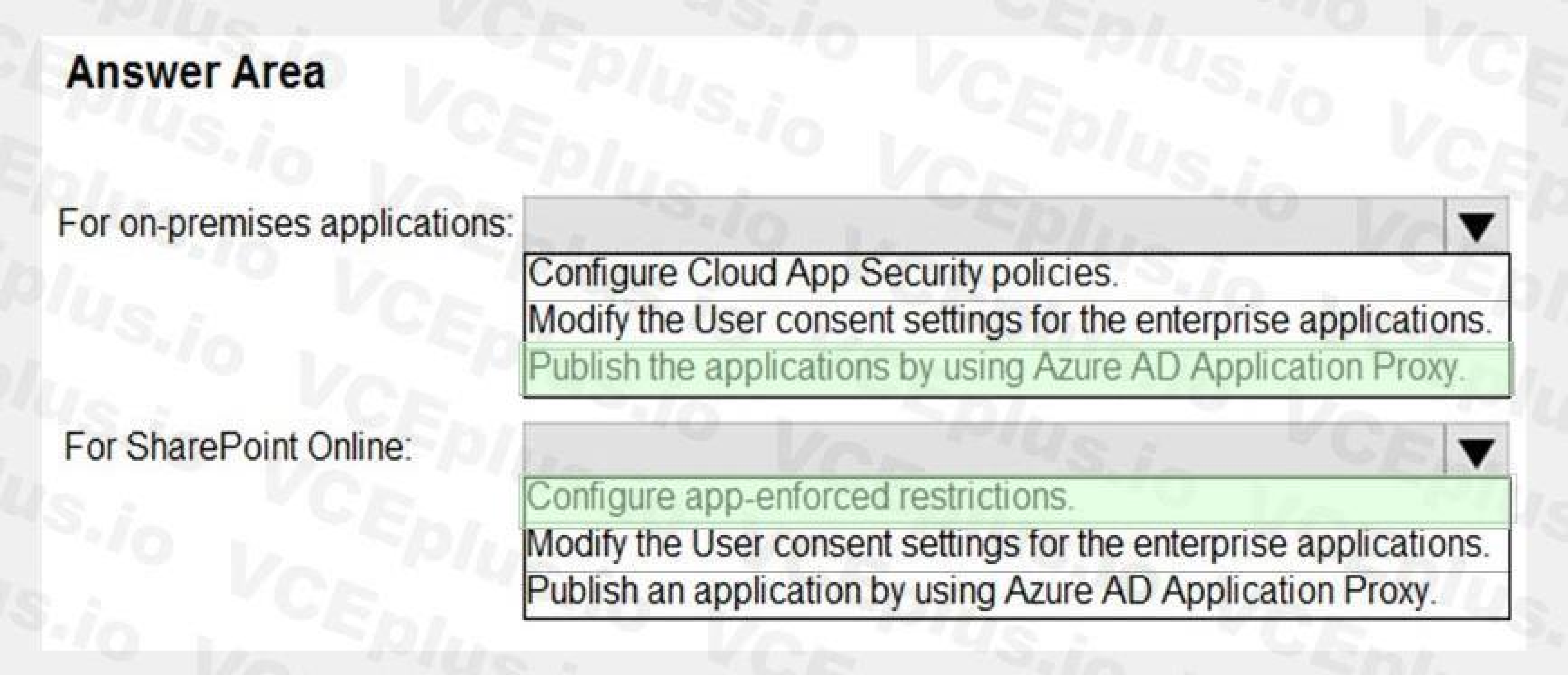


Answer Area

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.]

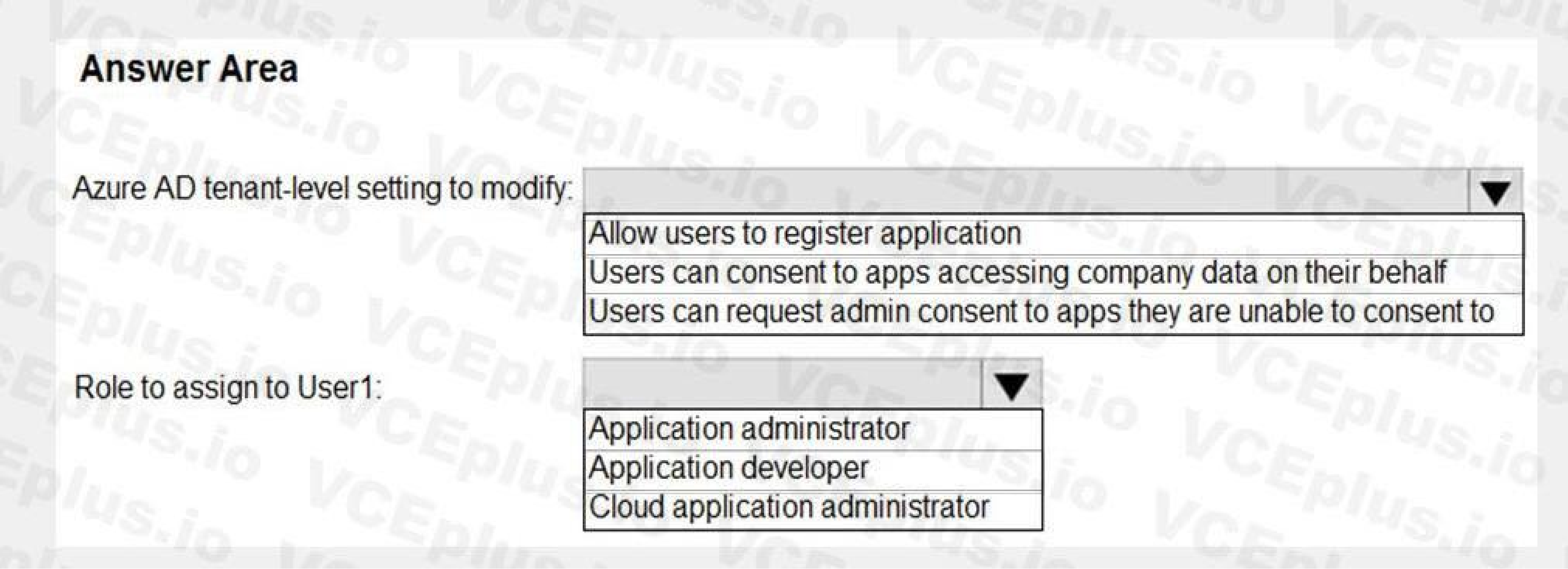
For SharePoint Online:

- [✓ 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 6
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

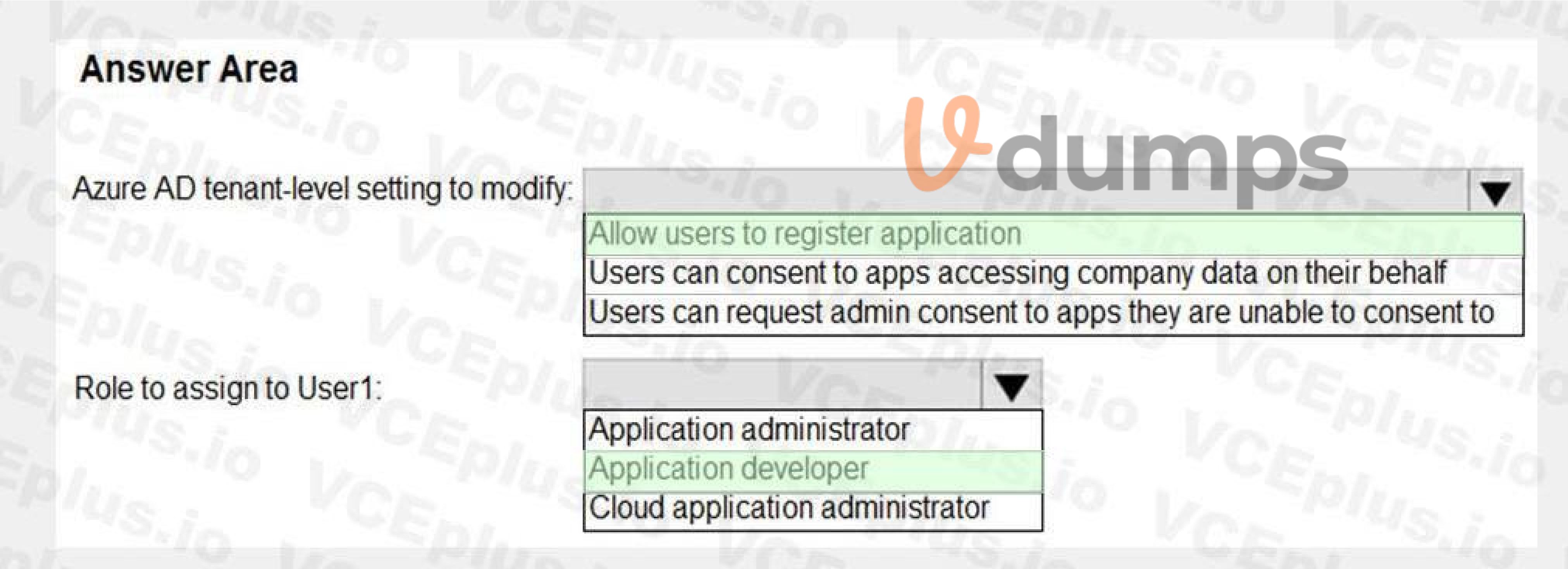
Azure AD tenant-level setting to modify:

- 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 7

HOTSPOT

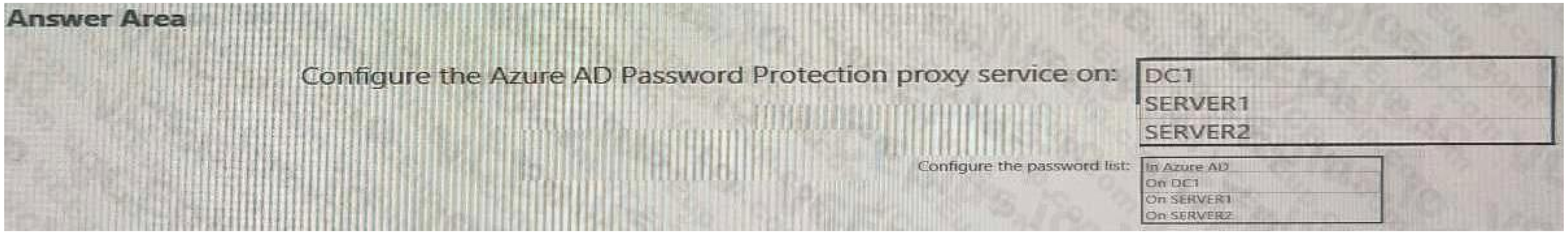
You need to implement password restrictions to meet the authentication requirements.

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

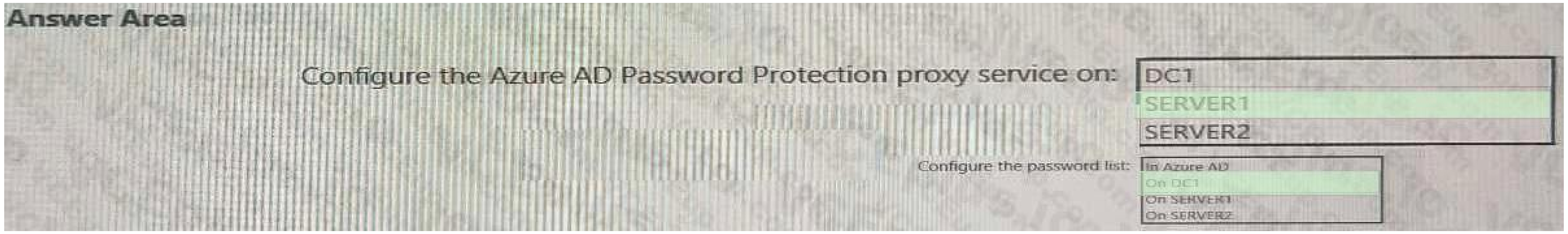
Configure the Azure AD Password Protection proxy service on:

- 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 8

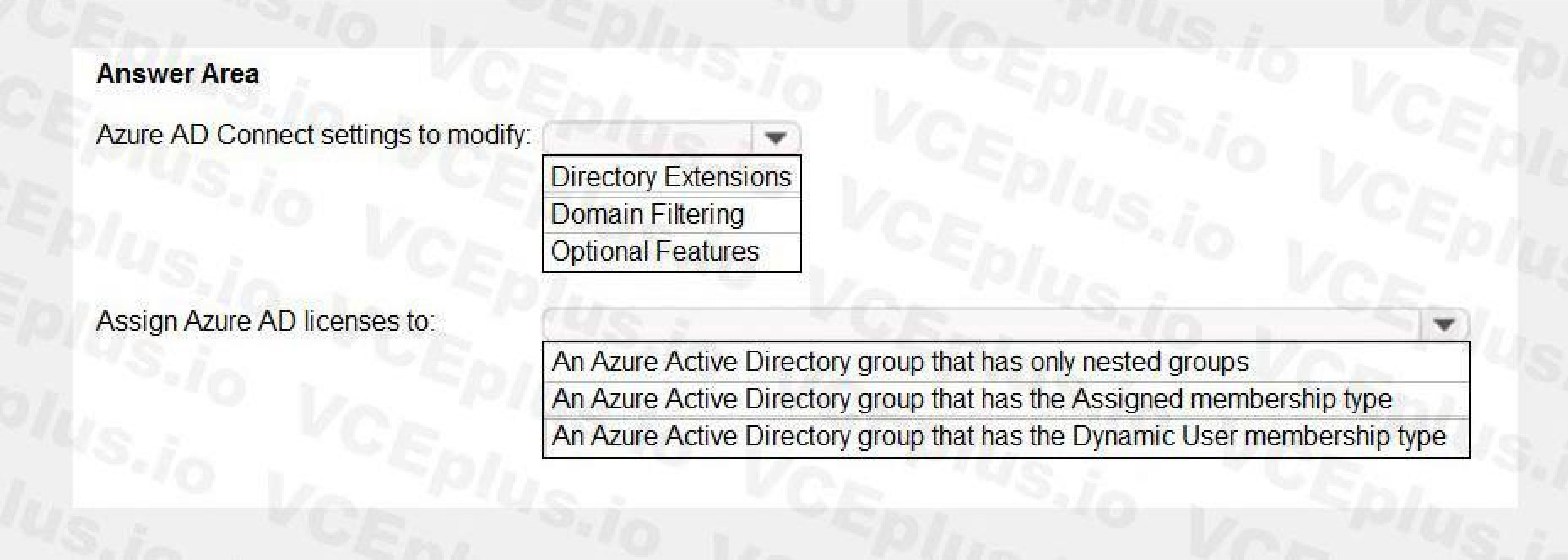
HOTSPOT

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

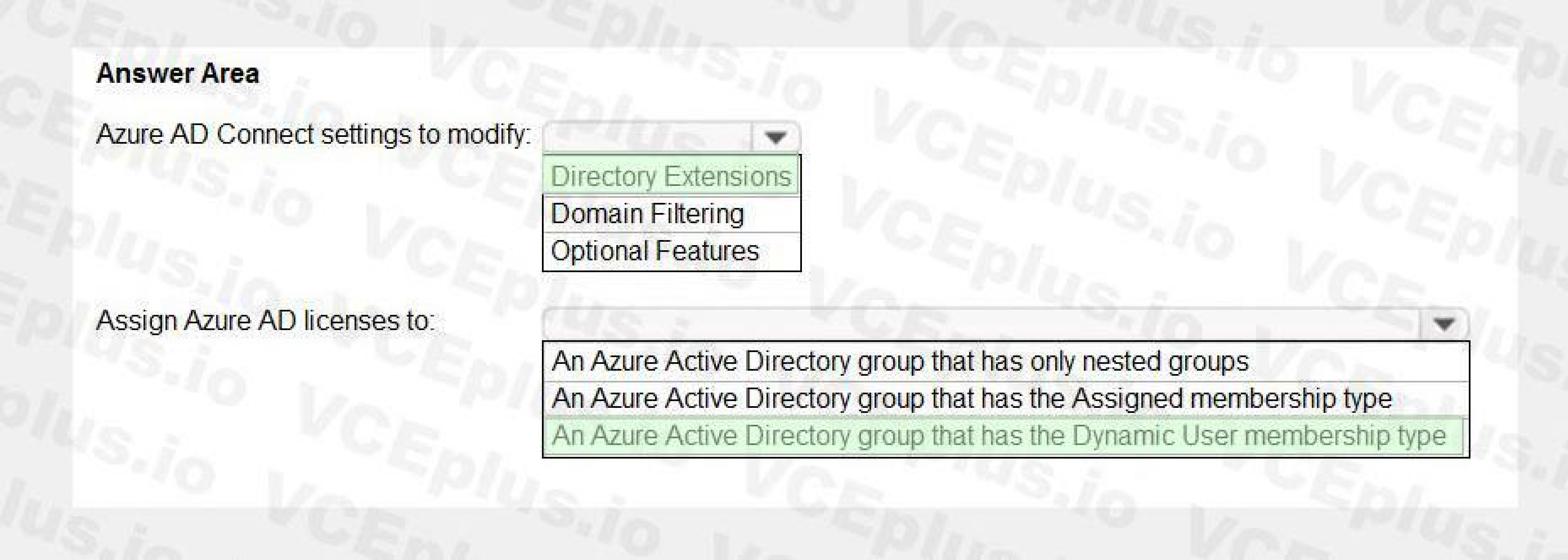
Azure AD Connect settings to modify:

- 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 9

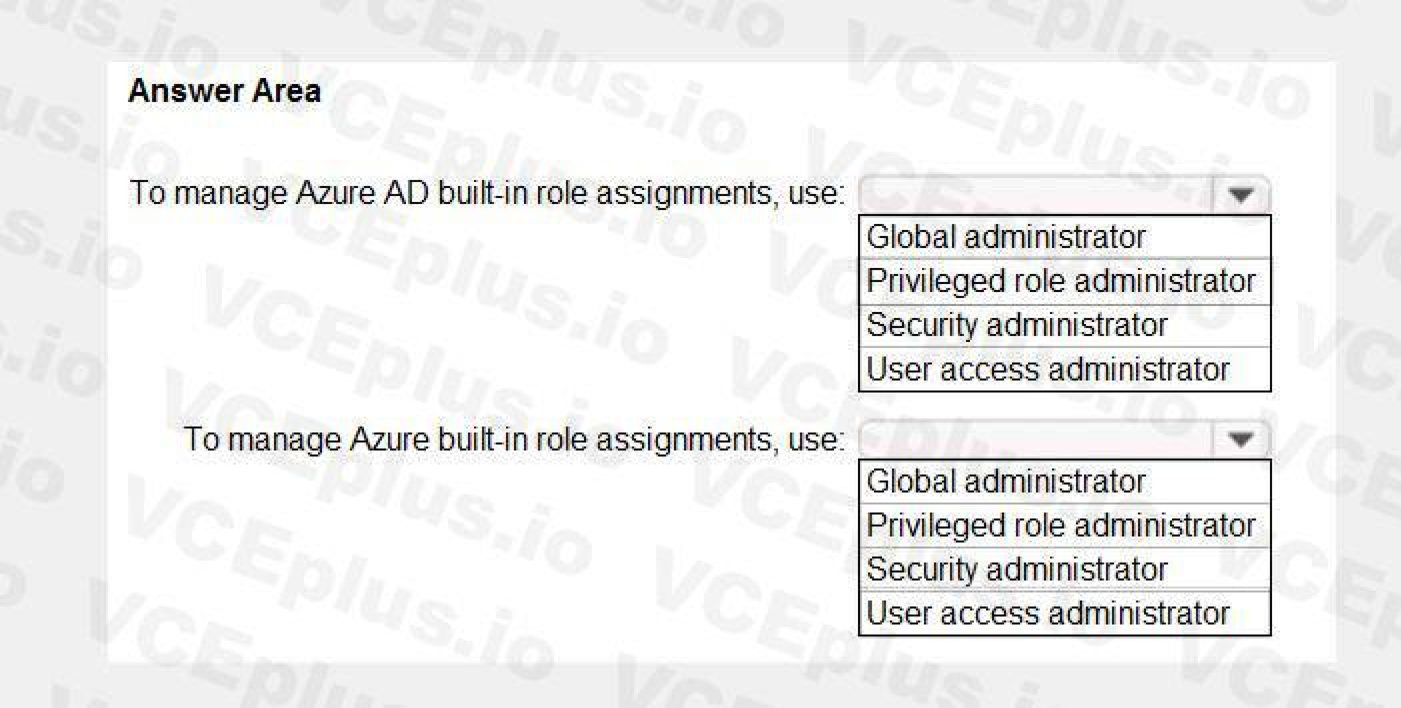
HOTSPOT

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

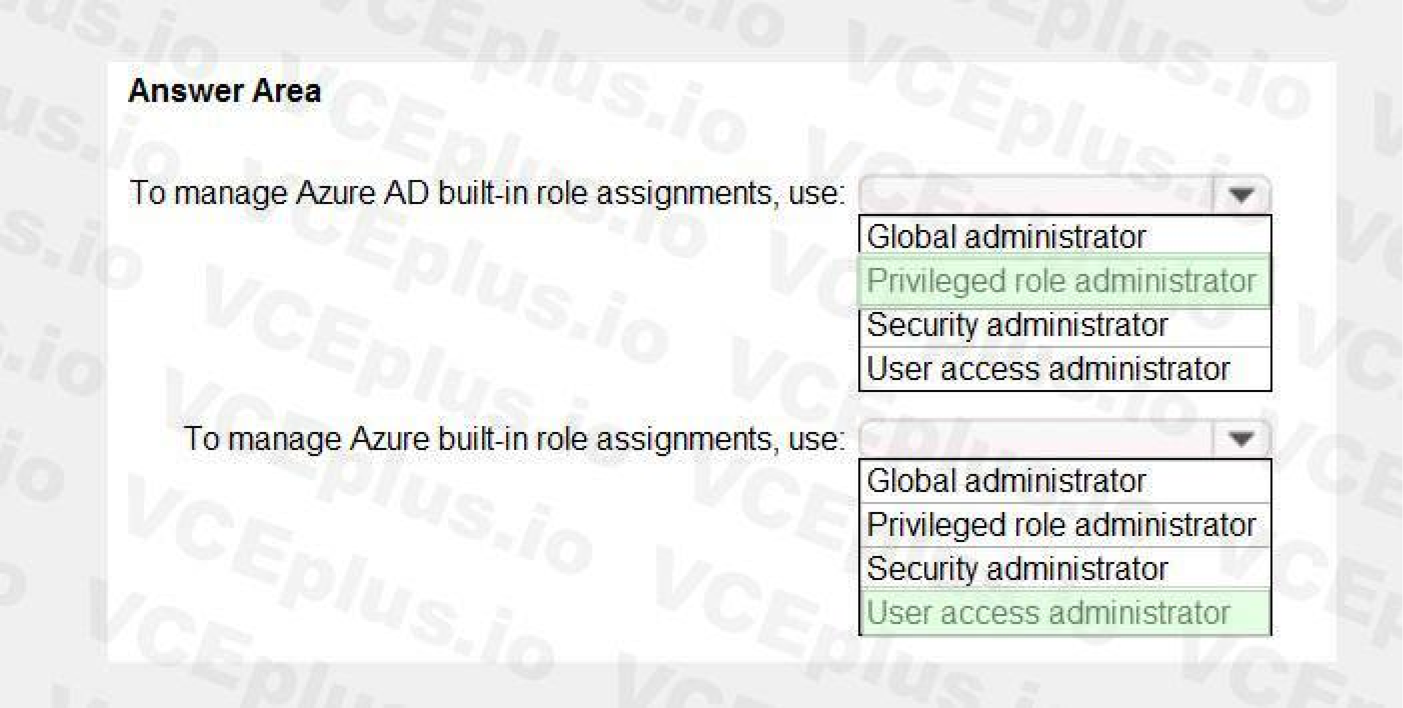
To manage Azure AD built-in role assignments, use:

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 10
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.

Exam C

QUESTION 1
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Active Directory forest that syncs to an Azure Active Directory (Azure AD) tenant.

You discover that when a user account is disabled in Active Directory, the disabled user can still authenticate to Azure AD for up to 30 minutes.
You need to ensure that when a user account is disabled in Active Directory, the user account is immediately prevented from authenticating to Azure AD.
Solution: You configure Azure AD Password Protection.
Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section:

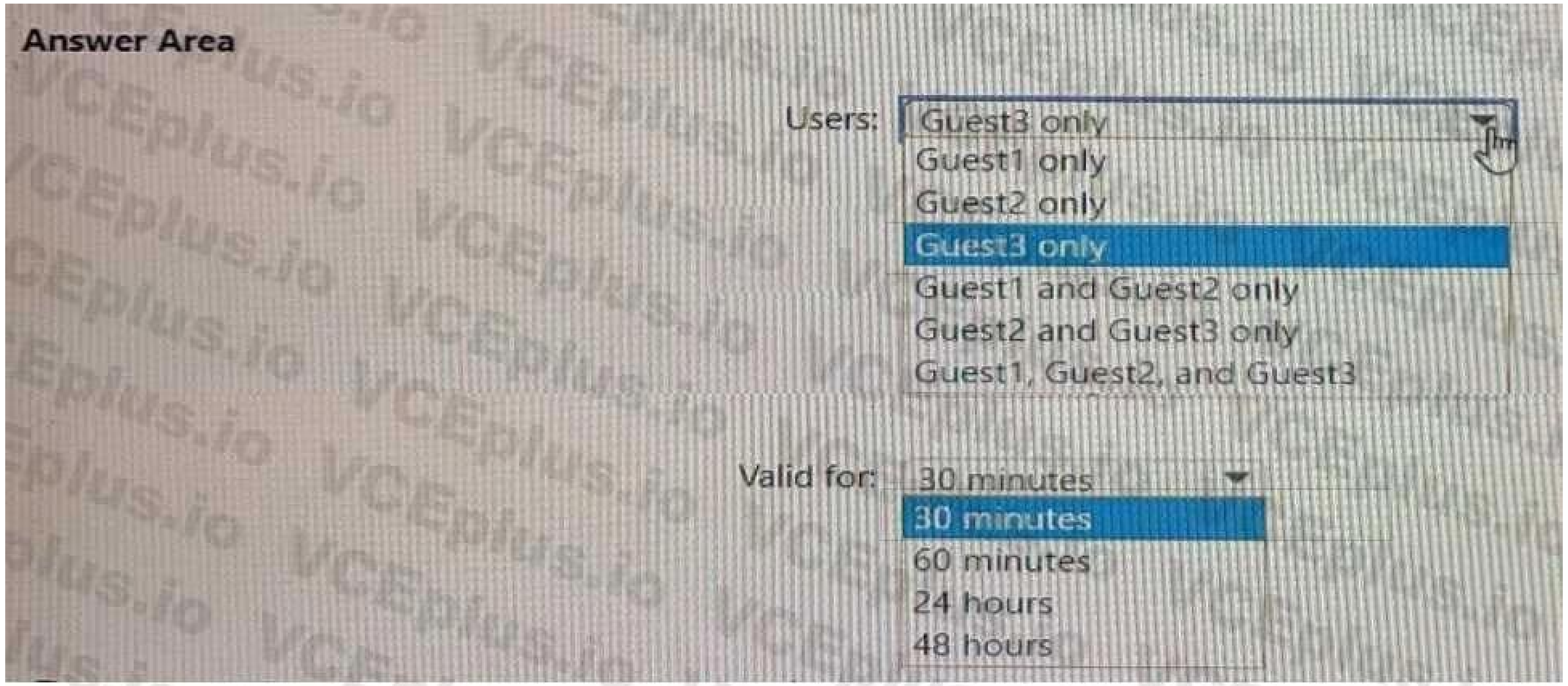
QUESTION 2
You have an Azure Active Directory (Azure AD) tenant named contoso.com.
You implement entitlement management to provide resource access to users at a company named Fabrikam, Inc. Fabrikam uses a domain named fabrikam.com.
Fabrikam users must be removed automatically from the tenant when access is no longer required.
You need to configure the following settings:
Block external user from signing in to this directory: No
Remove external user: Yes
Number of days before removing external user from this directory: 90
What should you configure on the Identity Governance blade?

A. Access packages
B. Settings
C. Terms of use
D. Access reviews

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

QUESTION 3
HOTSPOT
You have an Azure AD tenant named contoso.com that has Email one-time passcode for guests set to Yes.
You invite the guest users shown in the following table.
Which users will receive a one-time passcode, and how long will the passcode be valid? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

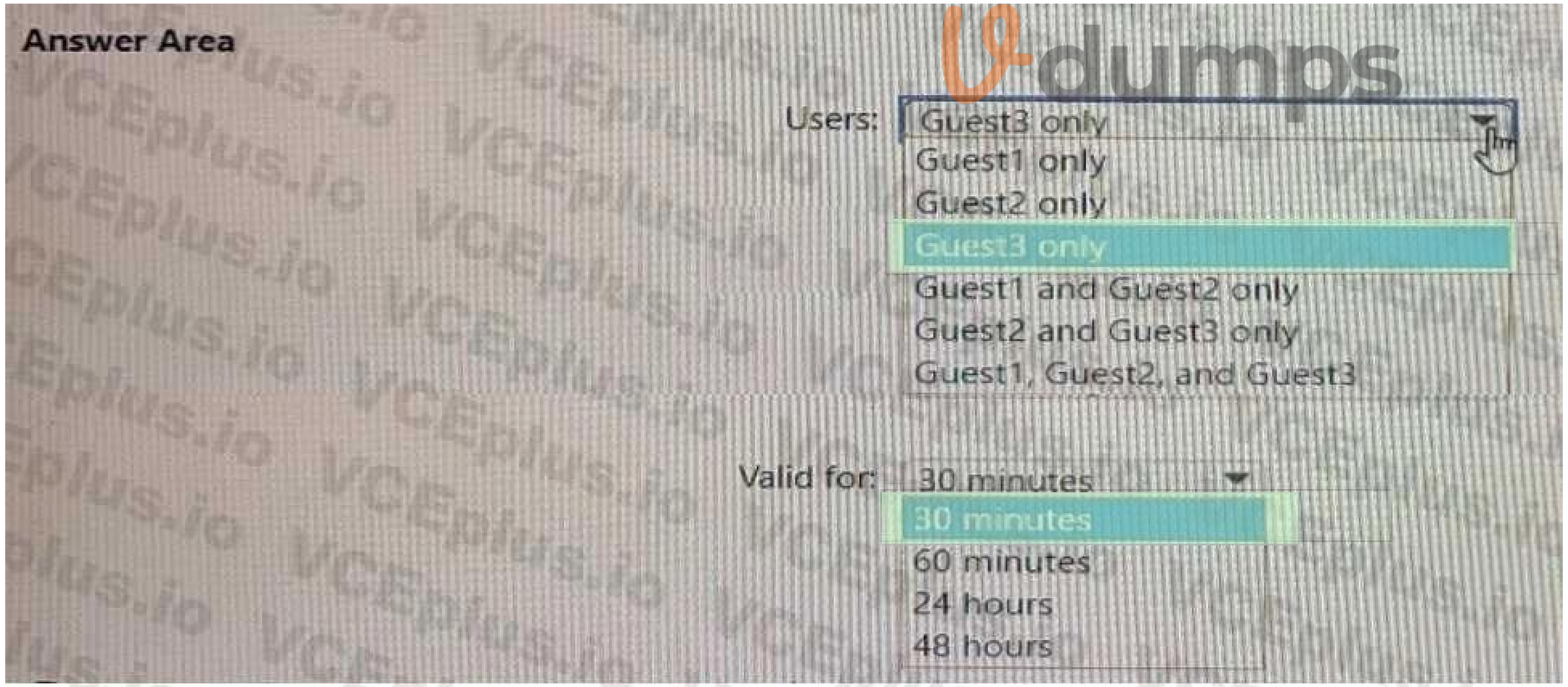
Users: Guest3 only

- Guest1 only
- Guest2 only
- Guest3 only
- Guest1 and Guest2 only
- Guest2 and Guest3 only
- Guest1, Guest2, and Guest3

Valid for: 30 minutes

- 30 minutes
- 60 minutes
- 24 hours
- 48 hours

Answer Area:



Answer Area

Users: Guest3 only

- Guest1 only
- Guest2 only
- [✓ Guest3 only]
- Guest1 and Guest2 only
- Guest2 and Guest3 only
- Guest1, Guest2, and Guest3

Valid for: 30 minutes

- [✓ 30 minutes]
- 60 minutes
- 24 hours
- 48 hours

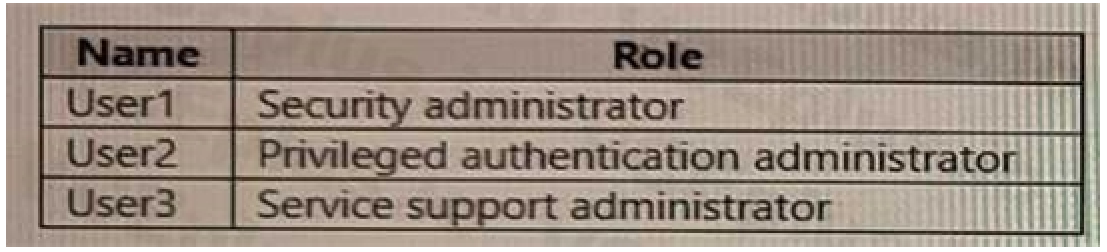
Section:

Explanation:

QUESTION 4

HOTSPOT

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



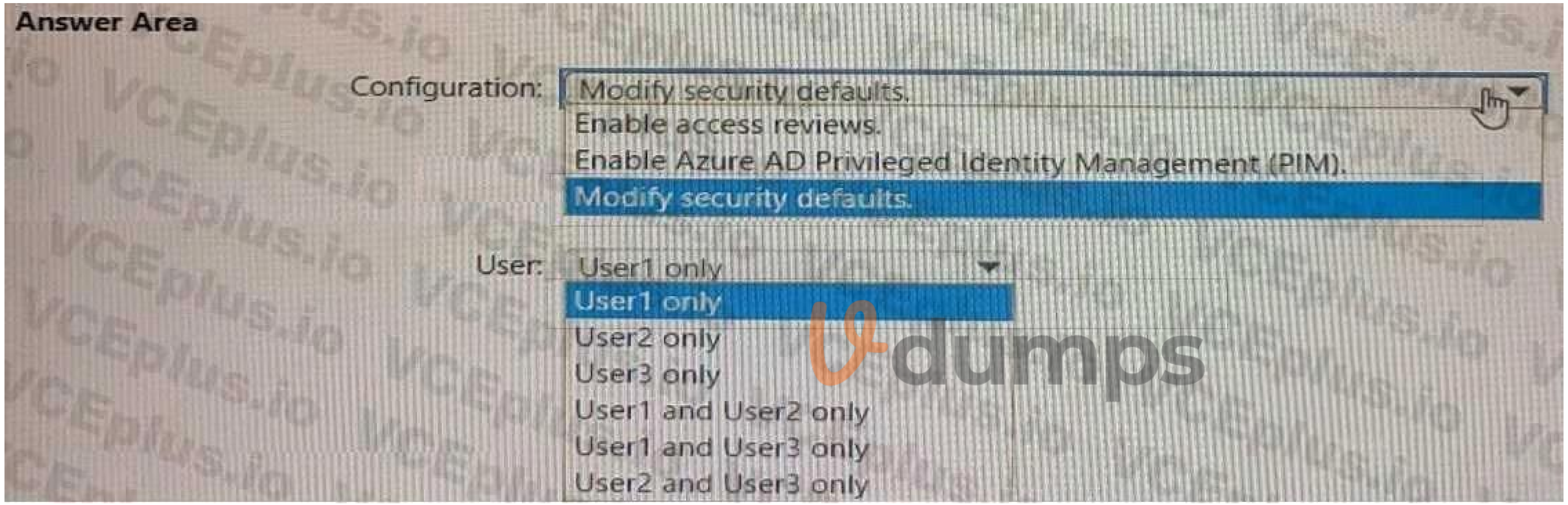
Name	Role
User1	Security administrator
User2	Privileged authentication administrator
User3	Service support administrator

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

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

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

Hot Area:

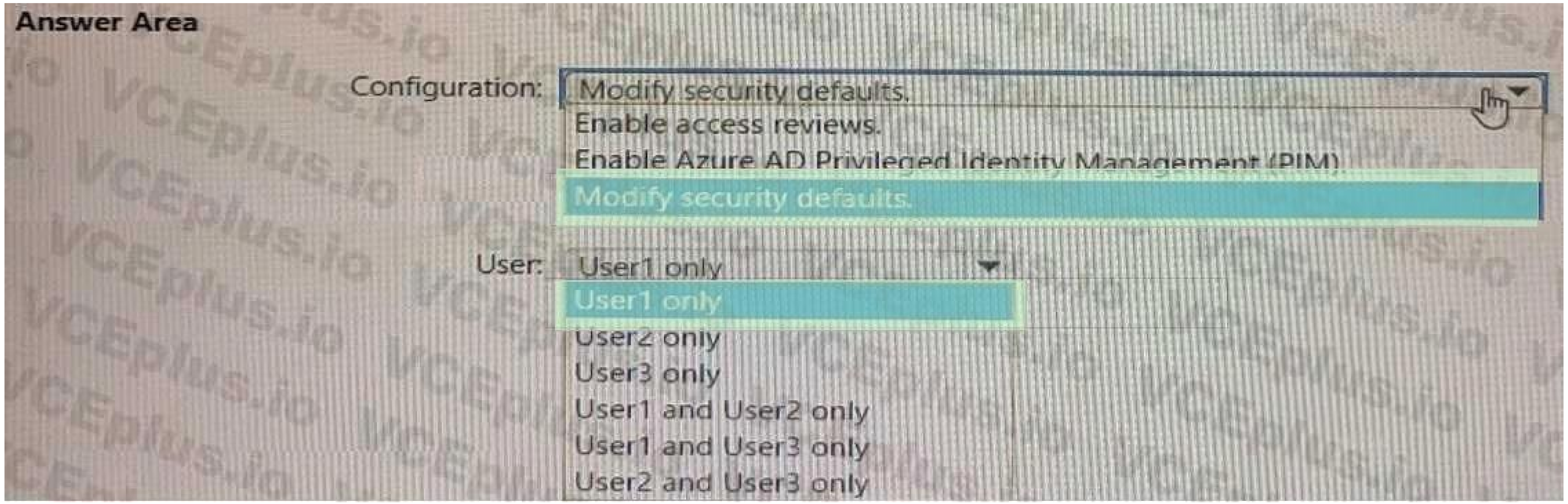


Answer Area

Configuration: Modify security defaults.

User: User1 only

Answer Area:



Answer Area

Configuration: Modify security defaults.

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

User: User1 only

- User1 only
- User2 only
- User3 only
- User1 and User2 only
- User1 and User3 only
- User2 and User3 only

Section:
Explanation:

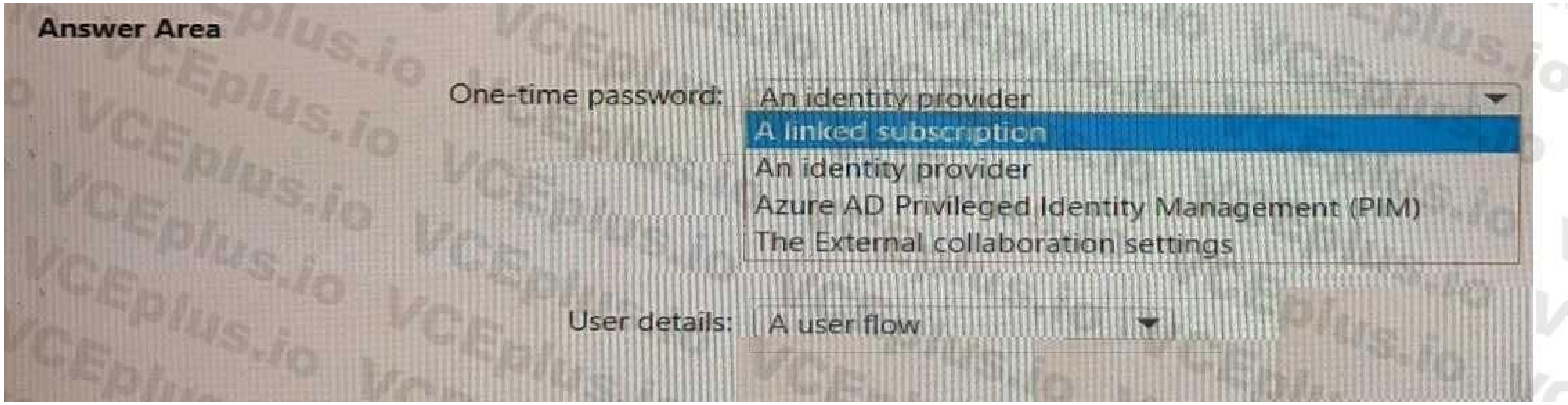
QUESTION 5
Your network contains an on-premises Active Directory domain that syncs to an Azure AD tenant.
Users sign in to computers that run Windows 10 and are joined to the domain.
You plan to implement Azure AD Seamless Single Sign-On (Azure AD Seamless SSO).
You need to configure the Windows 10 computers to support Azure AD Seamless SSO.
What should you do?

A. Modify the Local intranet zone settings
B. Configure Sign-in options from the Settings app.
C. Enable Enterprise State Roaming.
D. Install the Azure AD Connect Authentication Agent.

Correct Answer: B
Section:

QUESTION 6
HOTSPOT
You have an Azure AD tenant and an Azure web app named App1.
You need to provide guest users with self-service sign-up for App1. The solution must meet the following requirements:
• Guest users must be able to sign up by using a one-time password.
• The users must provide their first name, last name, city, and email address during the sign-up process.
What should you configure in the Azure Active Directory admin center for each requirement? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



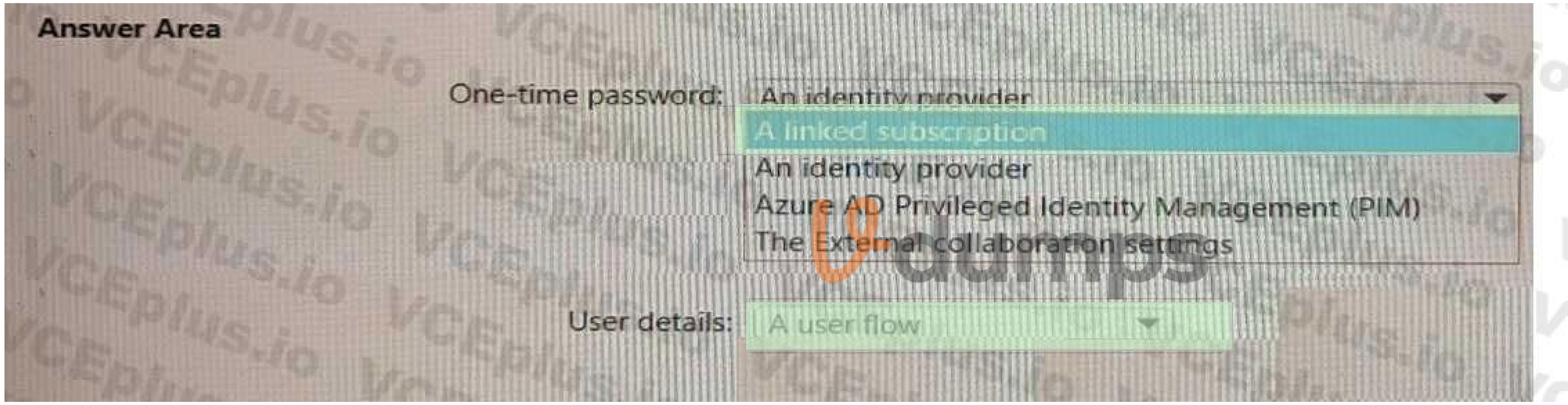
Answer Area

One-time password: An identity provider

- A linked subscription
- An identity provider
- Azure AD Privileged Identity Management (PIM)
- The External collaboration settings

User details: A user flow

Answer Area:



Answer Area

One-time password: An identity provider

- A linked subscription
- An identity provider
- Azure AD Privileged Identity Management (PIM)
- The External collaboration settings

User details: A user flow

Section:

Explanation:

QUESTION 7

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

You need to review the Azure AD sign-in logs to investigate sign-ins that occurred in the past.

For how long does Azure AD store events in the sign-in logs?

A. 14 days

B. 30 days

C. 90 days

D. 365 days

Correct Answer: B

Section:

Explanation:

Reference:

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

QUESTION 8
You have an Azure Active Directory (Azure AD) tenant.
For the tenant. Users can register applications Is set to No.
A user named Admin1 must deploy a new cloud app named App1.
You need to ensure that Admin1 can register App1 in Azure AD. The solution must use the principle of least privilege.
Which role should you assign to Admin1?

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

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

QUESTION 9
Your company requires that users request access before they can access corporate applications.
You register a new enterprise application named MyApp1 in Azure Active Dilatory (Azure AD) and configure single sign-on (SSO) for MyApp1.
Which settings should you configure next for MyApp1?

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

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

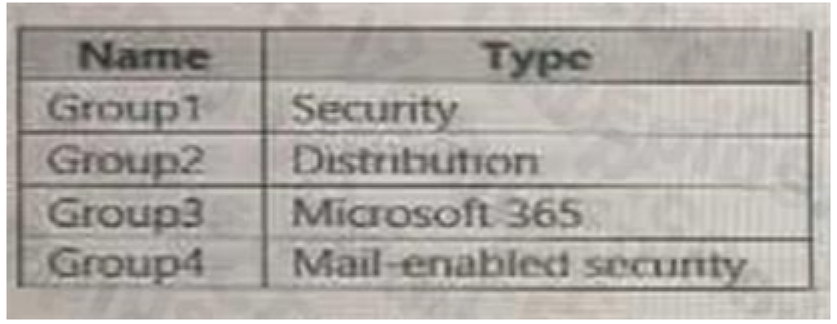
QUESTION 10
You have an Azure Active Directory (Azure AD) tenant.
You create an enterprise application collection named HR Apps that has the following settings:
• Applications: Appl. App?, App3
• Owners: Admin 1
• Users and groups: HRUsers
AH three apps have the following Properties settings:
• Enabled for users to sign in: Yes
• User assignment required: Yes
• Visible to users: Yes Users report that when they go to the My Apps portal, they only sue App1 and App2-You need to ensure that the users can also see App3. What should you do from App3?
What should you do from App3?

A. From Users and groups, add HRUsers.
B. Prom Properties, change User assignment required to No.

C. From Permissions, review the User consent permissions.
D. From Single sign on, configure a sign-on method.

Correct Answer: A
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-accessportal
https://docs.microsoft.com/en-us/azure/active-directory/user-help/my-applications-portalworkspaces

QUESTION 11
You have a Microsoft 365 tenant.
The Azure Active Directory (Azure AD) tenant contains the groups shown in the following table.



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

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

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

Correct Answer: A
Section:

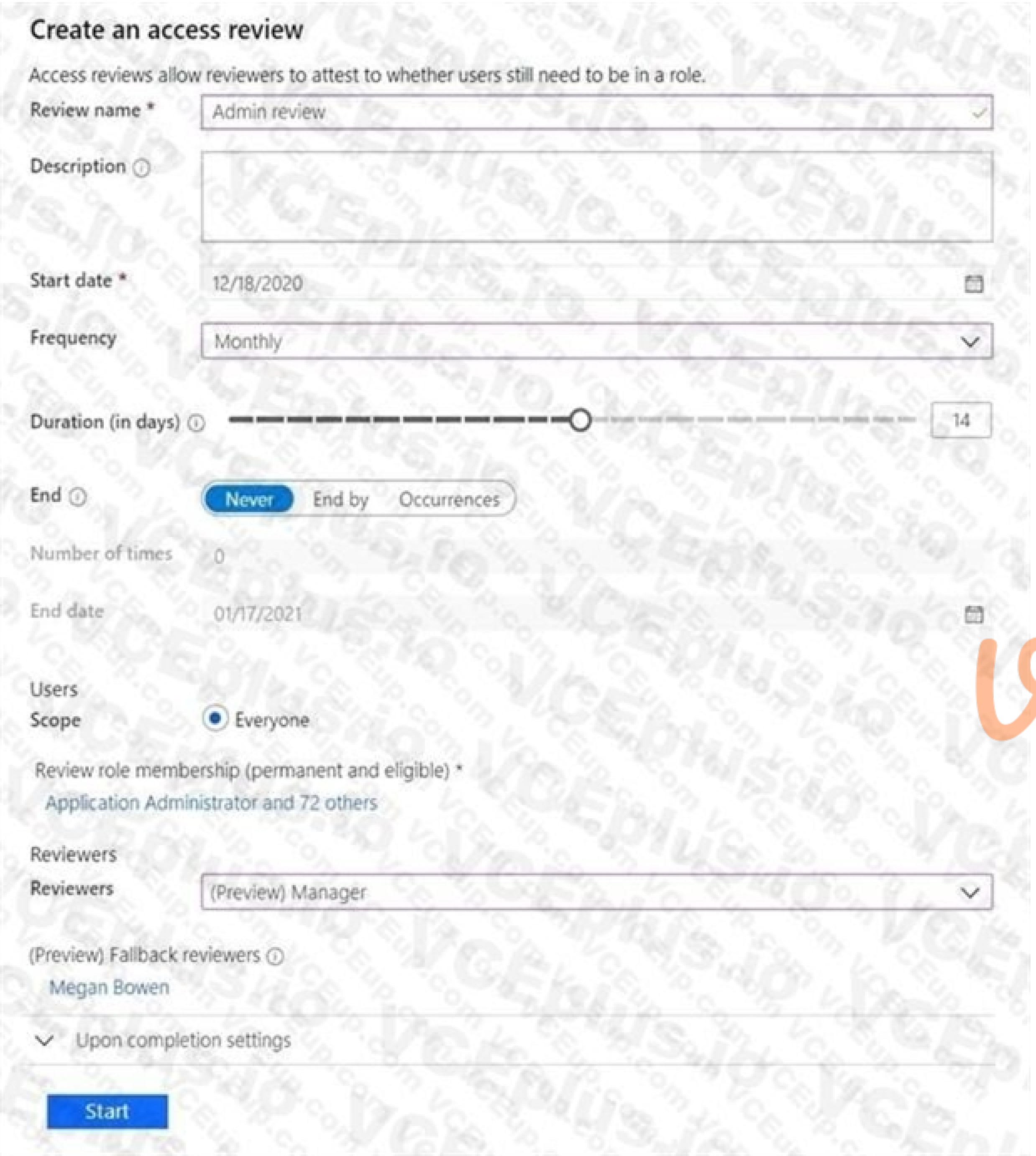
QUESTION 12
You configure a new Microsoft 36S tenant to use a default domain name of contosso.com.
You need to ensure that you can control access to Microsoft 365 resource-, by using conditional access policy.
What should you do first?

A. Disable the User consent settings.
B. Disable Security defaults.
C. Configure a multi-factor authentication (Ml A) registration policy1.
D. Configure password protection for Windows Server Active Directory.

Correct Answer: B
Section:

QUESTION 13
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have 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 add each manager as a fallback reviewer.
Does this meet the goal?

A. Yes

B. No

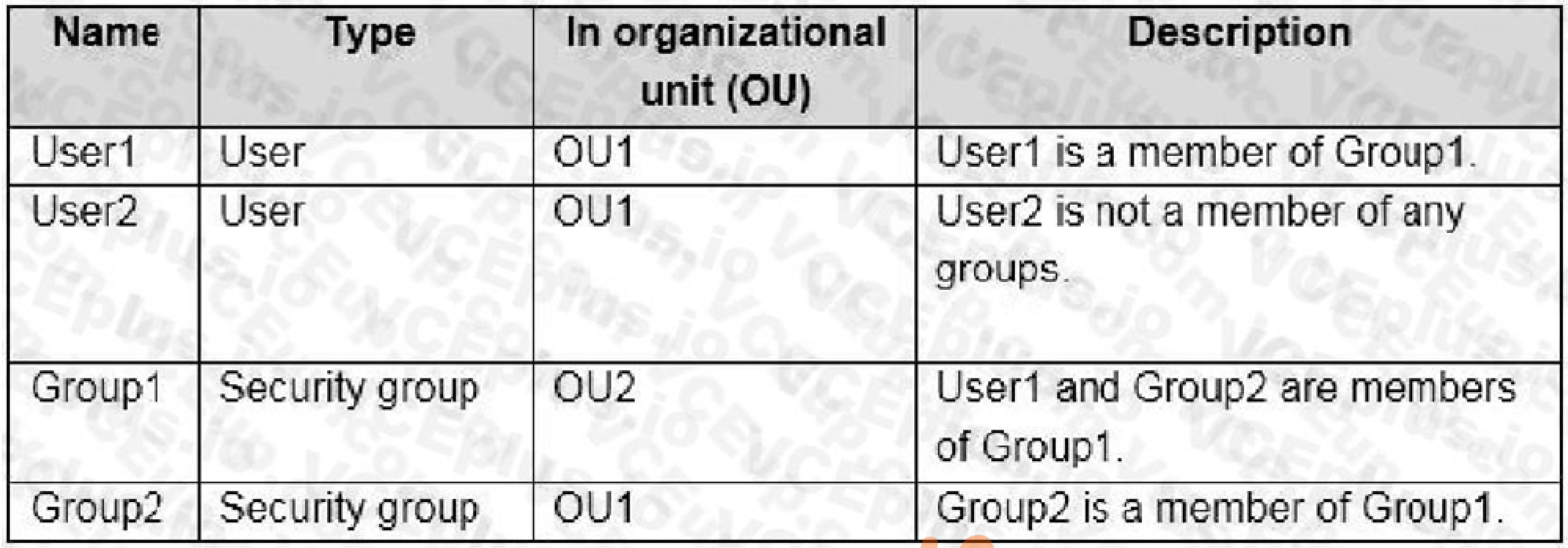
Correct Answer: B
Section:
Explanation:

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

QUESTION 14

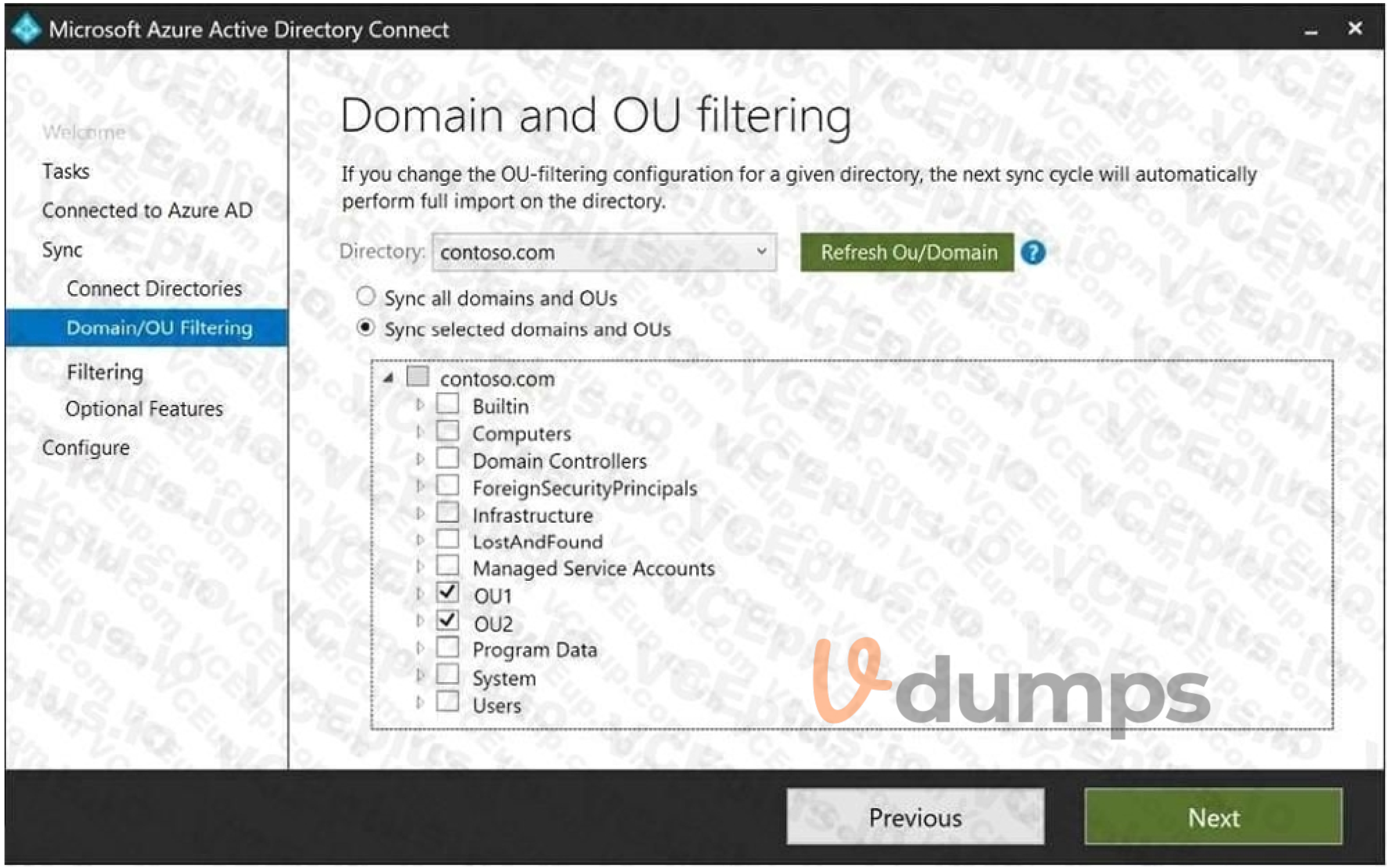
HOTSPOT

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



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

You install Azure AD Connect. You configure the Domain and OU filtering settings as shown in the Domain and OU Filtering exhibit. (Click the Domain and OU Filtering tab.)



Domain and OU filtering

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

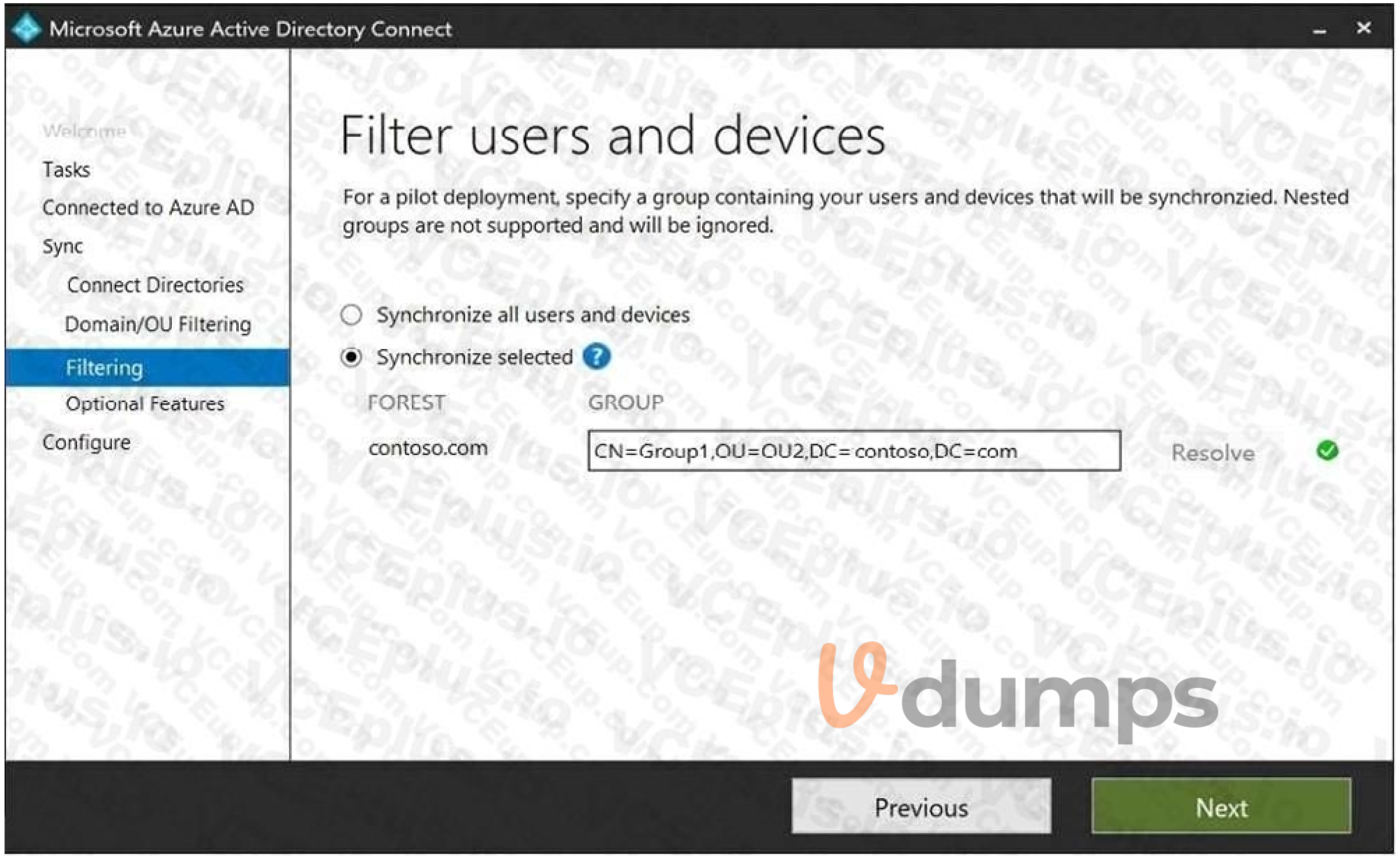
Directory: contoso.com

○ Sync all domains and OUs

● Sync selected domains and OUs

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

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



Filter users and devices

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

○ Synchronize all users and devices

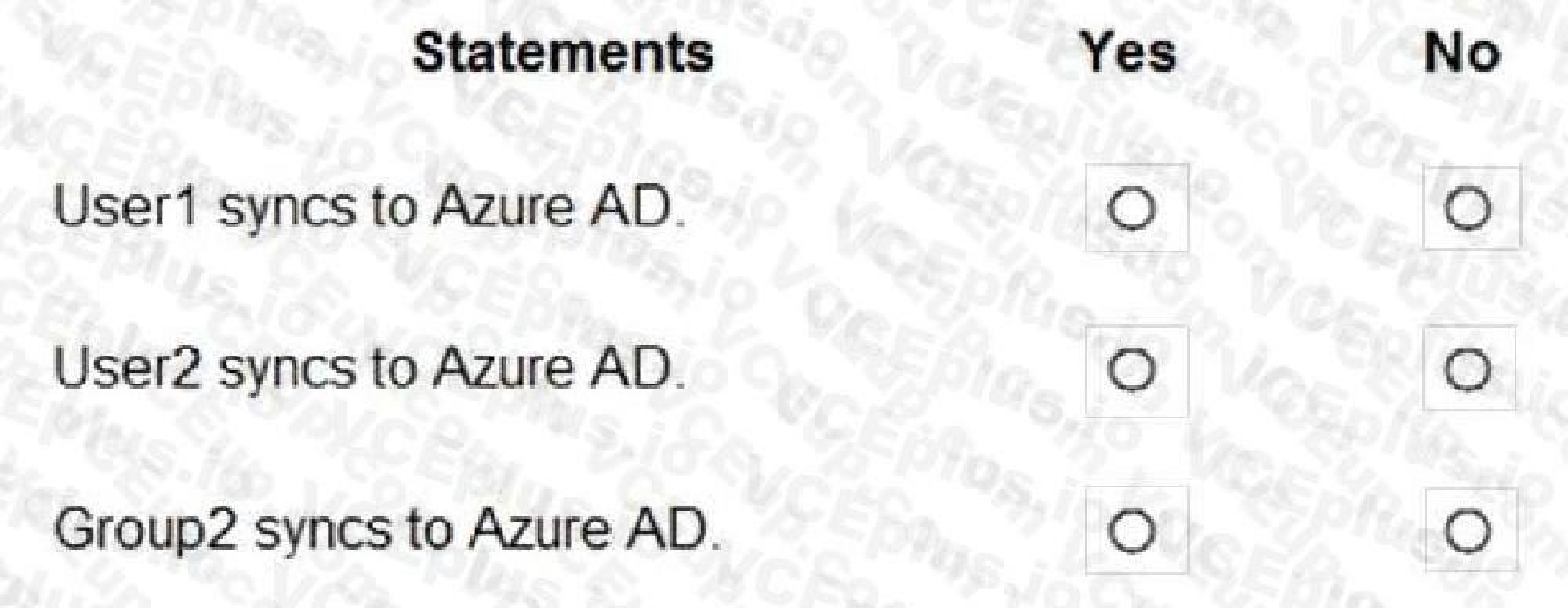
● Synchronize selected

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

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

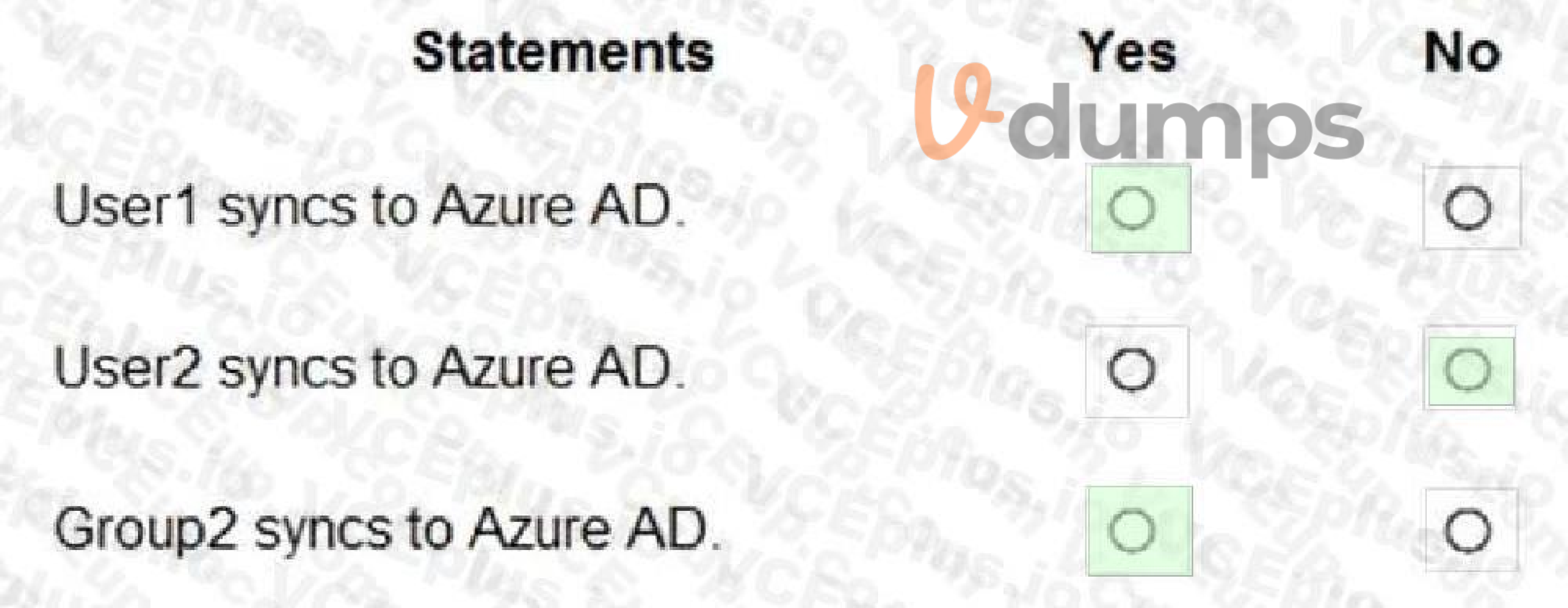
A.
B.
C.
D.

Hot Area:



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

Answer Area:



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

Section:
Explanation:
Only direct members of Group1 are synced. Group2 will sync as it is a direct member of Group1 but the members of Group2 will not sync.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-custom

QUESTION 15
You have a Microsoft 365 tenant.
All users have mobile phones and laptops.

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

A. a notification through the Microsoft Authenticator app
B. an app password
C. Windows Hello for Business
D. SMS

Correct Answer: C
Section:
Explanation:
In Windows 10, Windows Hello for Business replaces passwords with strong two-factor authentication on PCs and mobile devices. This authentication consists of a new type of user credential that is tied to a device and uses a biometric or
PIN.
After an initial two-step verification of the user during enrollment, Windows Hello is set up on the user's device and Windows asks the user to set a gesture, which can be a biometric, such as a fingerprint, or a PIN. The user provides the gesture to verify their identity. Windows then uses Windows Hello to authenticate users.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authenticationmethods
https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hellooverview

QUESTION 16

You have a Microsoft Entra tenant that has a Microsoft Entra ID P1 license.You need to review the Microsoft Entra ID sign-in logs to investigate sign-ins that occurred in the past. For how long does Microsoft Entra ID store events in the sign-in logs?

A. 14 days
B. 30 days
C. 90 days
D. 365 days

Correct Answer: B
Section:
Explanation:

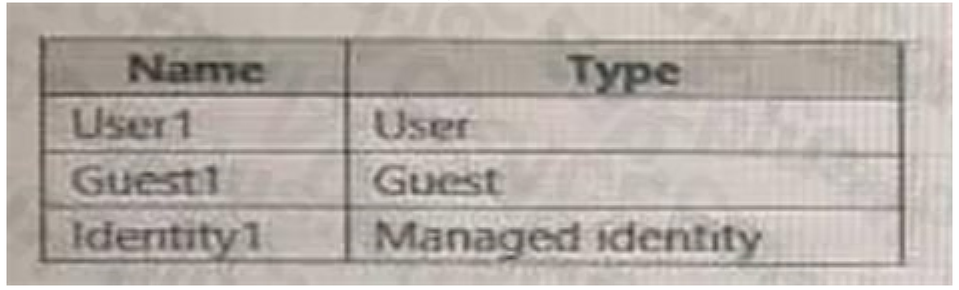
×End Practice TestAre you sure you want to end the test?YesNo

QUESTION 17
You have an Azure Active Directory (Azure AD) tenant named contoso.com that has Azure AD Identity Protection policies enforced.
You create an Azure Sentinel instance and configure the Azure Active Directory connector.
You need to ensure that Azure Sentinel can generate incidents based on the risk alerts raised by Azure AD Identity Protection.
What should you do first?

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

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

QUESTION 18
You have an Azure Active Directory (Azure AD) tenant that contains the objects shown in the following table.



Name	Type
User1	User
Guest1	Guest
Identity1	Managed identity

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

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

Correct Answer: D
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pimdeployment-plan

QUESTION 19
You have a Microsoft 365 tenant.
You need to ensure that you tan view Azure Active Directory (Azure AD) audit log information by using Azure Monitor.
What should you do first?

A. Run the Get-AzureADAuditDirectoryLogs cmdlet.
B. Create an Azure AD workbook.
C. Run the Set-AzureADTenantDetail cmdlet.
D. Modify the Diagnostics settings for Azure AD.

Correct Answer: A
Section:

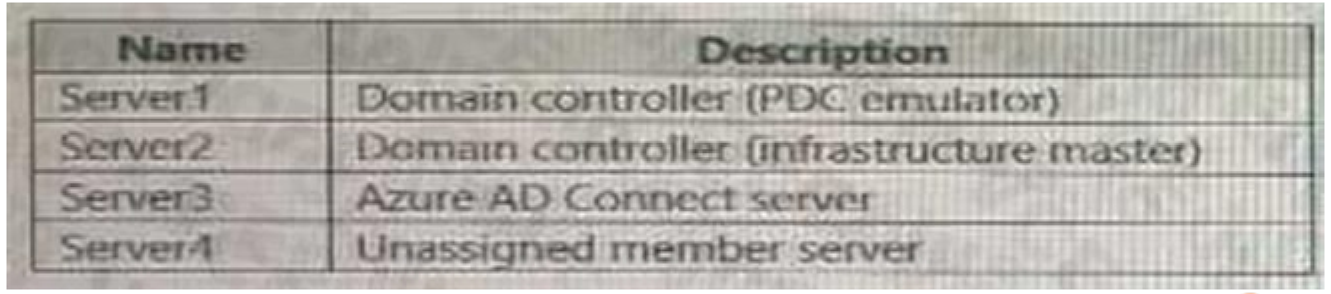
QUESTION 20
You have an Azure Active Directory (Azure AD) tenant named conto.so.com that has Azure AD Identity Protection enabled. You need to Implement a sign-in risk remediation policy without blocking access.
What should you do first?

A. Configure access reviews in Azure AD.
B. Enforce Azure AD Password Protection.
C. implement multi-factor authentication (MFA) for all users.

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

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

QUESTION 21
You have an Azure Active Directory (Azure AD) tenant that syncs to an Active Directory forest. The tenant-uses through authentication.
A corporate security policy states the following:
Domain controllers must never communicate directly to the internet.
Only required software must be- installed on servers.
The Active Directory domain contains the on-premises servers shown in the following table.



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

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

A. Server2
B. Server4
C. Server1
D. Server3

Correct Answer: C
Section:

QUESTION 22
You have an Azure Active Directory (Azure AD) tenant.
You configure self-service password reset (SSPR) by using the following settings:
- Require users to register when signing in: Yes
- Number of methods required to reset: 1

What is a valid authentication method available to users?

A. home prions
B. mobile app notification
C. a mobile app code
D. an email to an address in your organization

Correct Answer: C
Section:

QUESTION 23
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

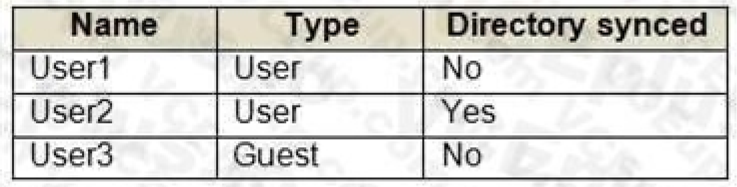
Correct Answer: B
Section:

QUESTION 24
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

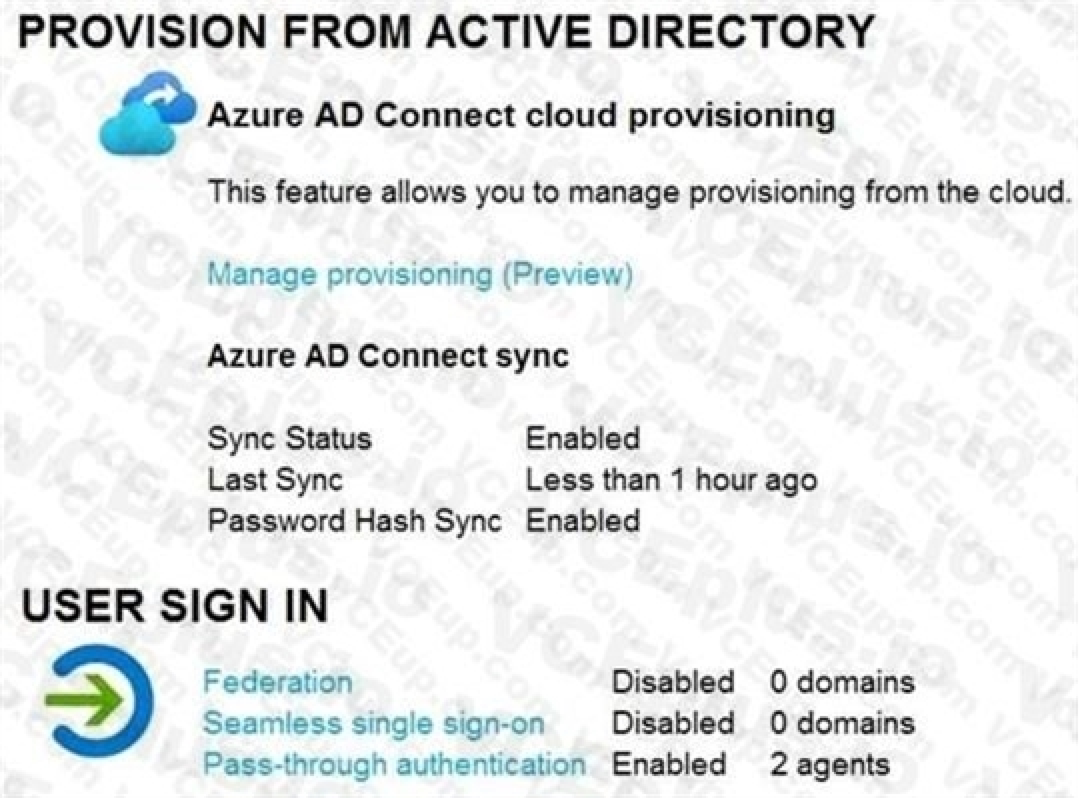
Correct Answer: B
Section:

QUESTION 25
Your network contains an on-premises Active Directory domain that syncs to an Azure Active Directory (Azure AD) tenant. The tenant contains the users shown in the following table.



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

All the users work remotely.
Azure AD Connect is configured in Azure AD as shown in the following exhibit.



PROVISION FROM ACTIVE DIRECTORY

Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

Manage provisioning (Preview)

Azure AD Connect sync

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

USER SIGN IN

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

Connectivity from the on-premises domain to the internet is lost.
Which users can sign in to Azure AD?

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

Correct Answer: B
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta-currentlimitations

QUESTION 26
You have a Microsoft 365 tenant.
All users have mobile phones and laptops.
The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity. While working from the remote locations, the users connect their laptop to a wired network that has internet access.
You plan to implement multi-factor authentication (MFA).
Which MFA authentication method can the users use from the remote location?

A. a notification through the Microsoft Authenticator app
B. email
C. security questions
D. a verification code from the Microsoft Authenticator app

Correct Answer: D

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

QUESTION 27
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You use Azure Monitor to analyze Azure Active Directory (Azure AD) activity logs.
You receive more than 100 email alerts each day for failed Azure AD user sign-in attempts.
You need to ensure that a new security administrator receives the alerts instead of you.
Solution: From Azure AD, you modify the Diagnostics settings.
Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section:

QUESTION 28
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains an Azure AD enterprise application named App1.
A contractor uses the credentials of user1@outlook.com.
You need to ensure that you can provide the contractor with access to App1. The contractor must be able to authenticate as user1@outlook.com.
What should you do?

A. Run the New-AzureADMSInvitation cmdlet.
B. Configure the External collaboration settings.
C. Add a WS-Fed identity provider.
D. Implement Azure AD Connect.

Correct Answer: A
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-addguest-users-portal
https://docs.microsoft.com/en-us/powershell/module/azuread/newazureadmsinvitation?view=azureadps-2.0

QUESTION 29
You have 2,500 users who are assigned Microsoft Office 365 Enterprise E3 licenses. The licenses are assigned to individual users.
From the Groups blade in the Azure Active Directory admin center, you assign Microsoft 365 Enterprise E5 licenses to the users.
You need to remove the Office 365 Enterprise E3 licenses from the users by using the least amount of administrative effort.
What should you use?

A. the Administrative units blade in the Azure Active Directory admin center
B. the Set-AzureAdUser cmdlet
C. the Groups blade in the Azure Active Directory admin center

D. the Sec-MsolUserLicense cmdlet

Correct Answer: C
Section:
Explanation:

QUESTION 30
You have an Azure Active Directory (Azure AD) tenant that contains cloud-based enterprise apps.
You need to group related apps into categories in the My Apps portal.
What should you create?

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

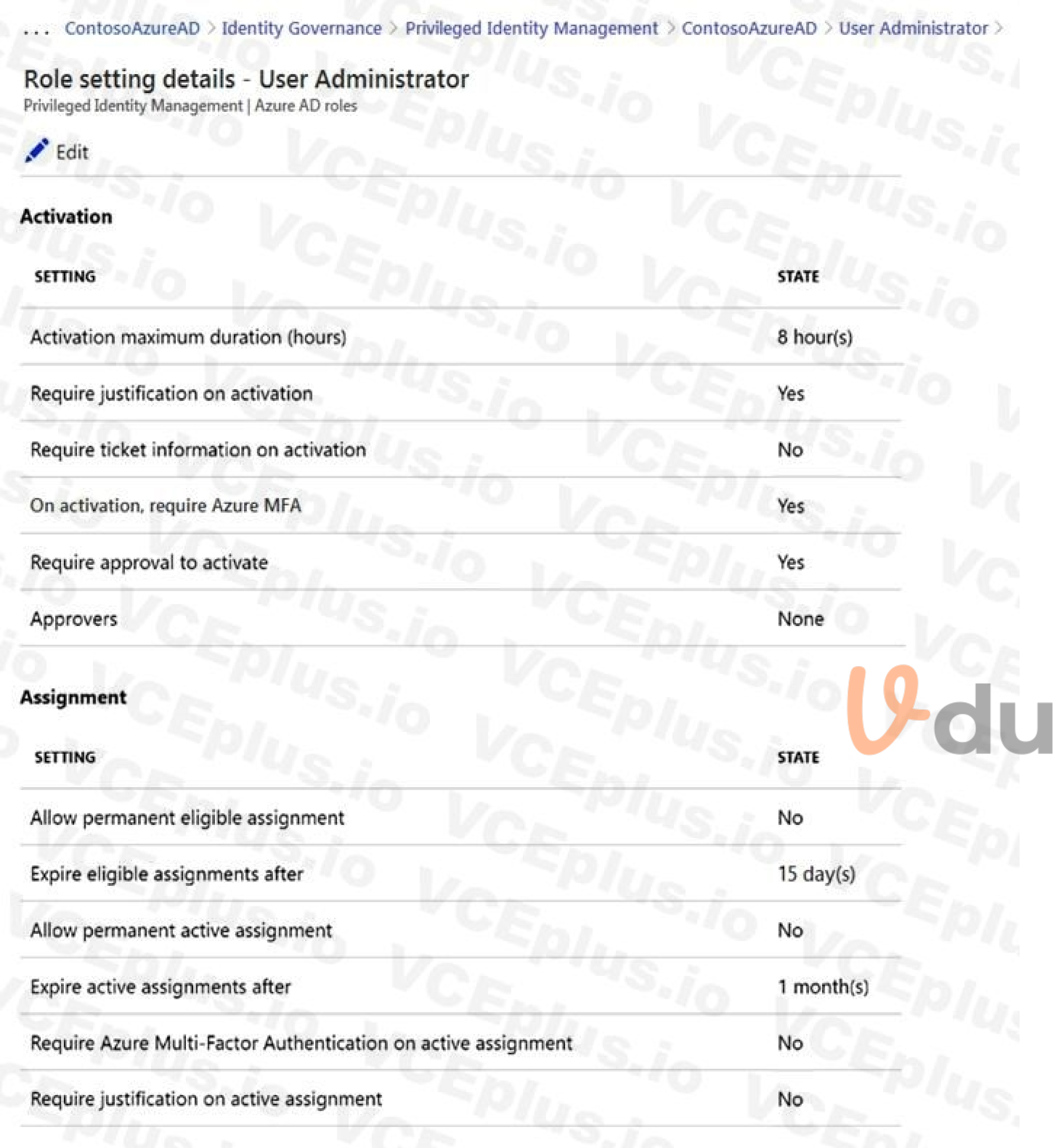
Correct Answer: B
Section:
Explanation:
Reference:
https://support.microsoft.com/en-us/account-billing/customize-app-collections-in-the-my-appsportal-2dae6b8a-d8b0-4a16-9a5d-71ed4d6a6c1d

QUESTION 31
You have an Azure Active Directory Premium P2 tenant.
You create a Log Analytics workspace.
You need to ensure that you can view Azure Active Directory (Azure AD) audit log information by using Azure Monitor.
What should you do first?

A. Run the Set-AzureADTenantDetail cmdlet.
B. Create an Azure AD workbook.
C. Modify the Diagnostics settings for Azure AD.
D. Run the Get-AzureADAuditDirectoryLogs cmdlet.

Correct Answer: D
Section:
Explanation:

QUESTION 32
HOTSPOT
You have an Azure Active Directory (Azure AD) tenant that contains Azure AD Privileged Identity Management (PIM) role settings for the User administrator role as shown in the following exhibit.



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

Role setting details - User Administrator

Privileged Identity Management | Azure AD roles

Activation

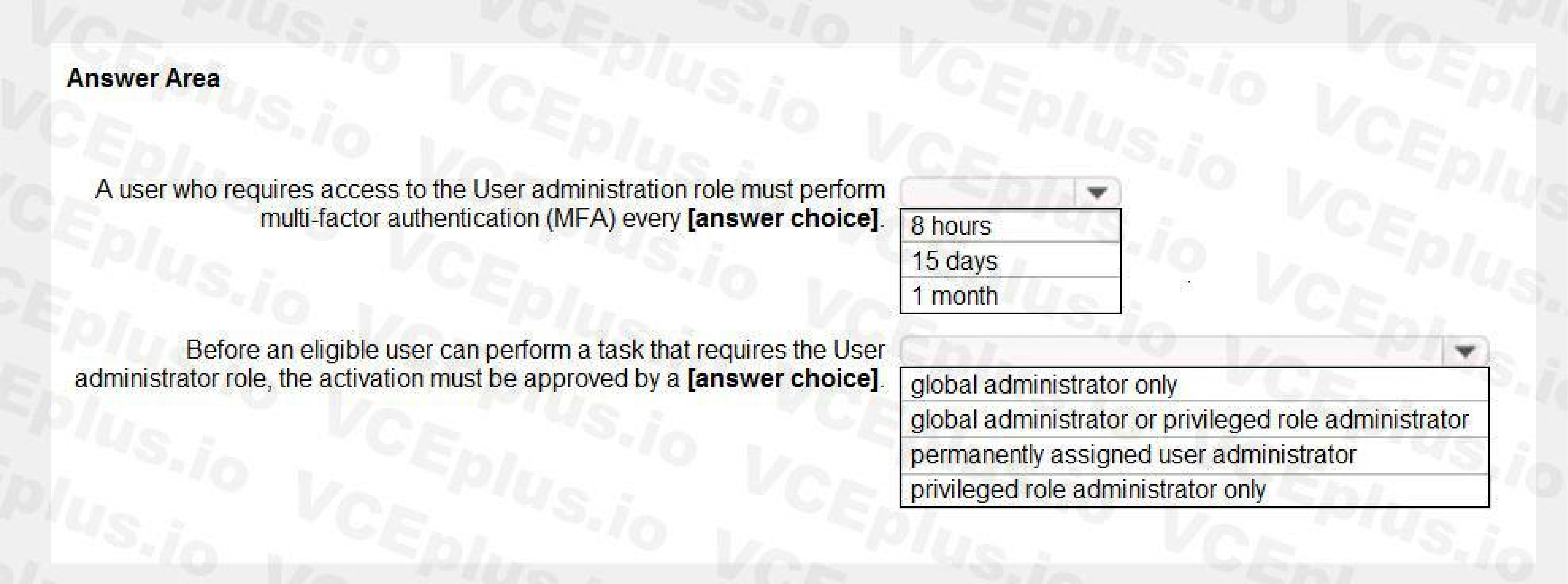
SETTING	STATE
Activation maximum duration (hours)	8 hour(s)
Require justification on activation	Yes
Require ticket information on activation	No
On activation, require Azure MFA	Yes
Require approval to activate	Yes
Approvers	None

Assignment

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

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

Hot Area:



Answer Area

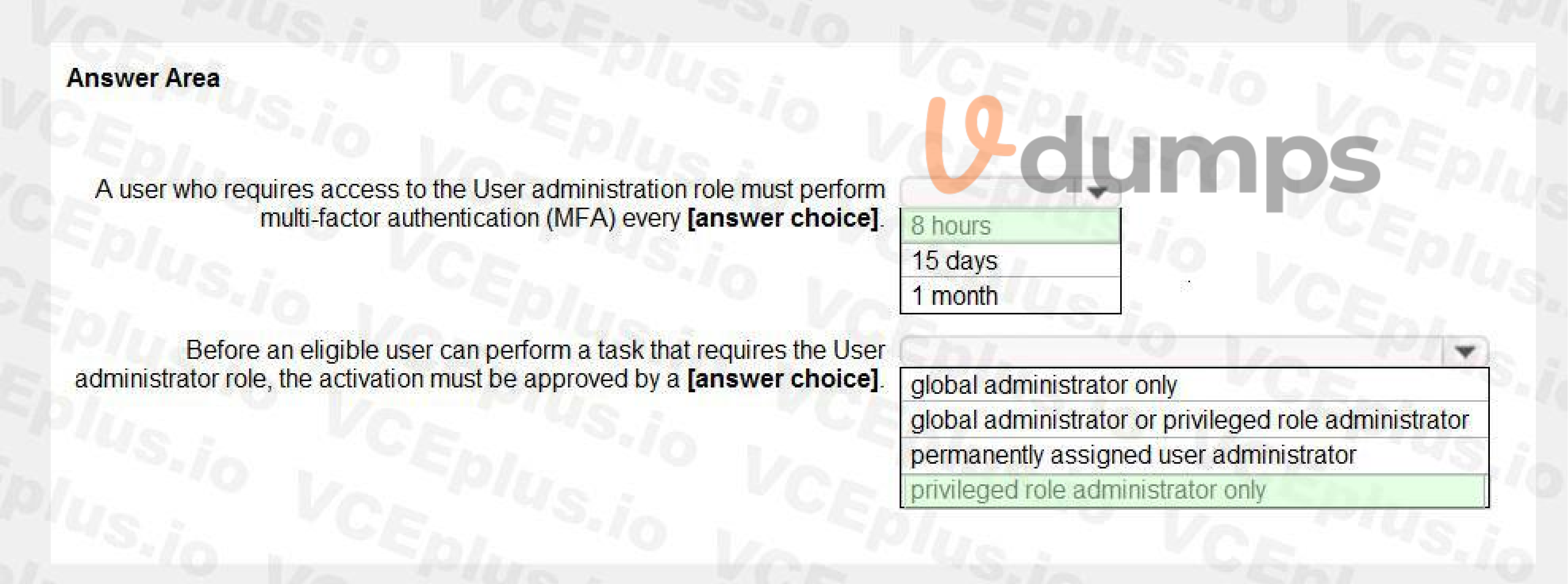
A user who requires access to the User administration role must perform multi-factor authentication (MFA) every **[answer choice]**.

- 8 hours
- 15 days
- 1 month

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

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

Answer Area:



Answer Area

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

- [✓ 8 hours]
- 15 days
- 1 month

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

- global administrator only
- global administrator or privileged role administrator
- permanently assigned user administrator
- [✓ privileged role administrator only]

Section:

Explanation:

Reference:

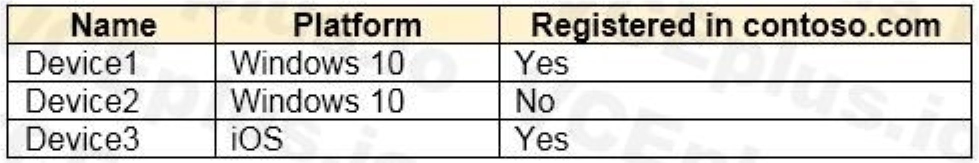
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-deployment-plan

QUESTION 33

HOTSPOT

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

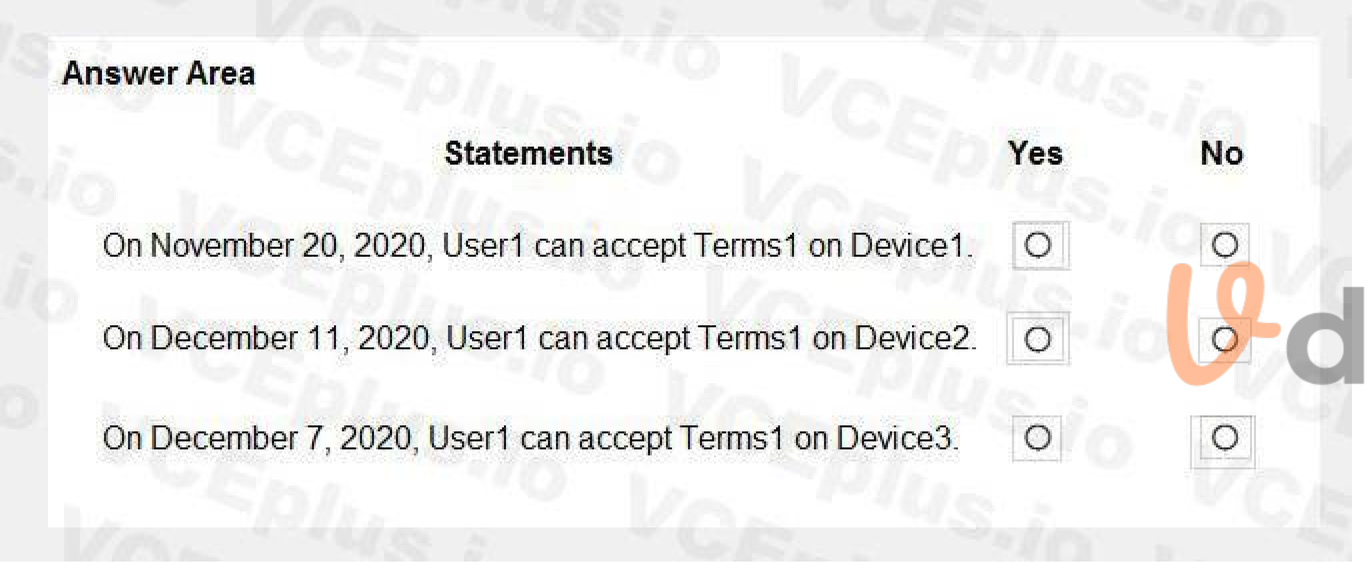
User1 has the devices shown in the following table.



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

On November 5, 2020, you create and enforce terms of use in contoso.com that has the following settings:
Name: Terms1
Display name: Contoso terms of use
Require users to expand the terms of use: On
Require users to consent on every device: On
Expire consents: On
Expire starting on: December 10, 2020
Frequency: Monthly
On November 15, 2020, User1 accepts Terms1 on Device3.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

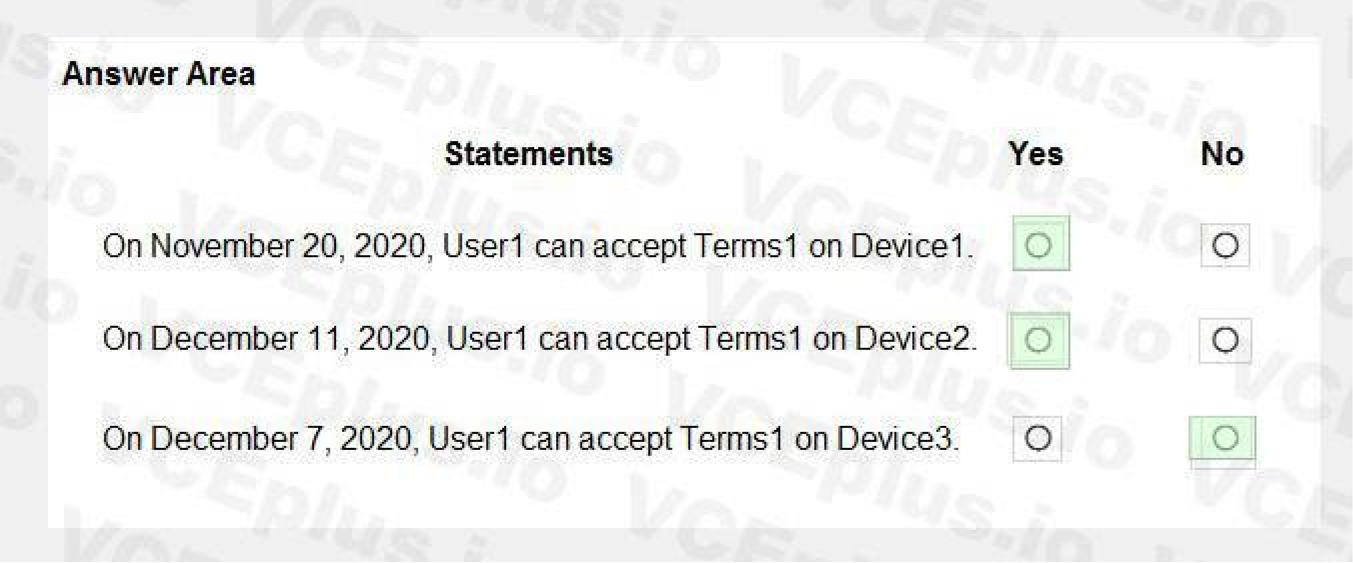
Hot Area:



Answer Area

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

Answer Area:



Answer Area

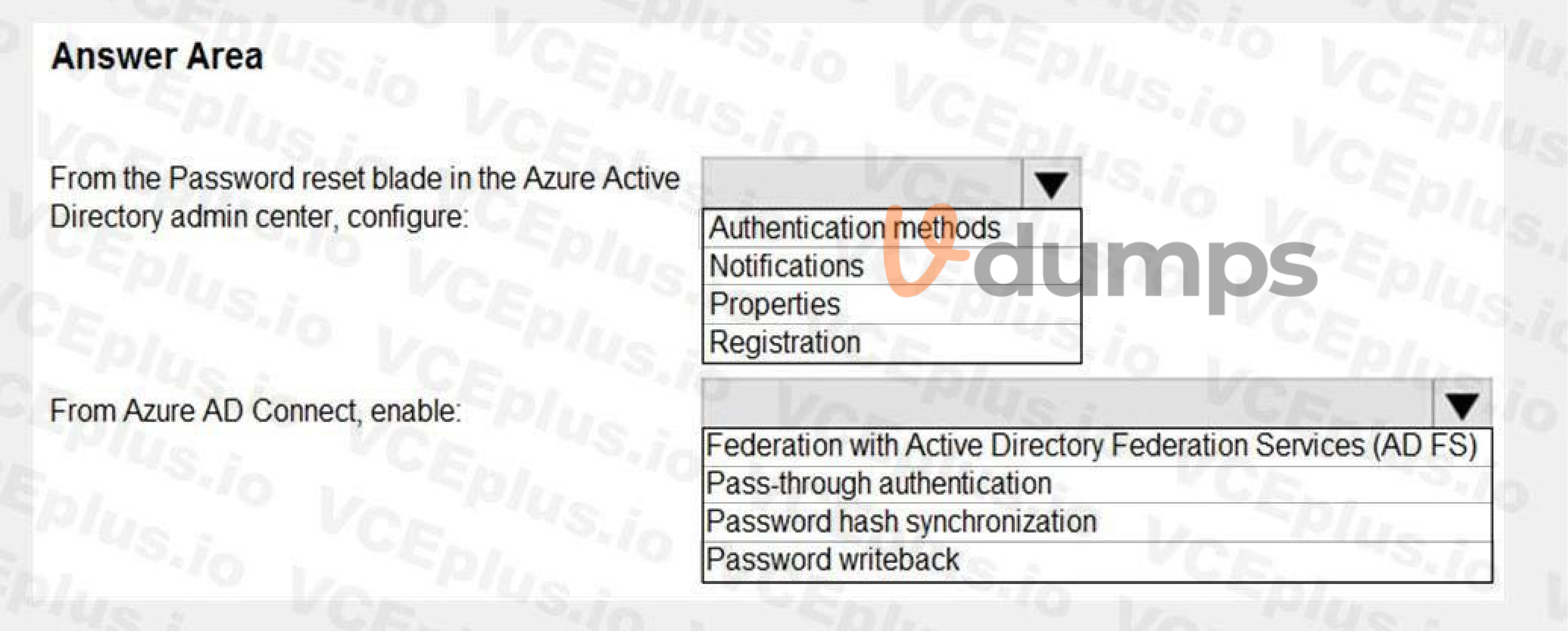
Statements	Yes	No
On November 20, 2020, User1 can accept Terms1 on Device1.	[✓ ○]	○
On December 11, 2020, User1 can accept Terms1 on Device2.	[✓ ○]	○
On December 7, 2020, User1 can accept Terms1 on Device3.	○	[✓ ○]

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

Box 2: Yes because User1 has not yet accepted the terms on Device2. User1 will be prompted to register the device before the terms can be accepted.
Box 3: No because User1 has already accepted the terms on Device3. The terms do not expire until December 10th and then monthly after that.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use

QUESTION 34
HOTSPOT
You have a Microsoft 365 tenant and an Active Directory domain named adatum.com.
You deploy Azure AD Connect by using the Express Settings.
You need to configure self-service password reset (SSPR) to meet the following requirements:
When users reset their password, they must be prompted to respond to a mobile app notification or answer three predefined security questions.
Passwords must be synced between the tenant and the domain regardless of where the password was reset.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

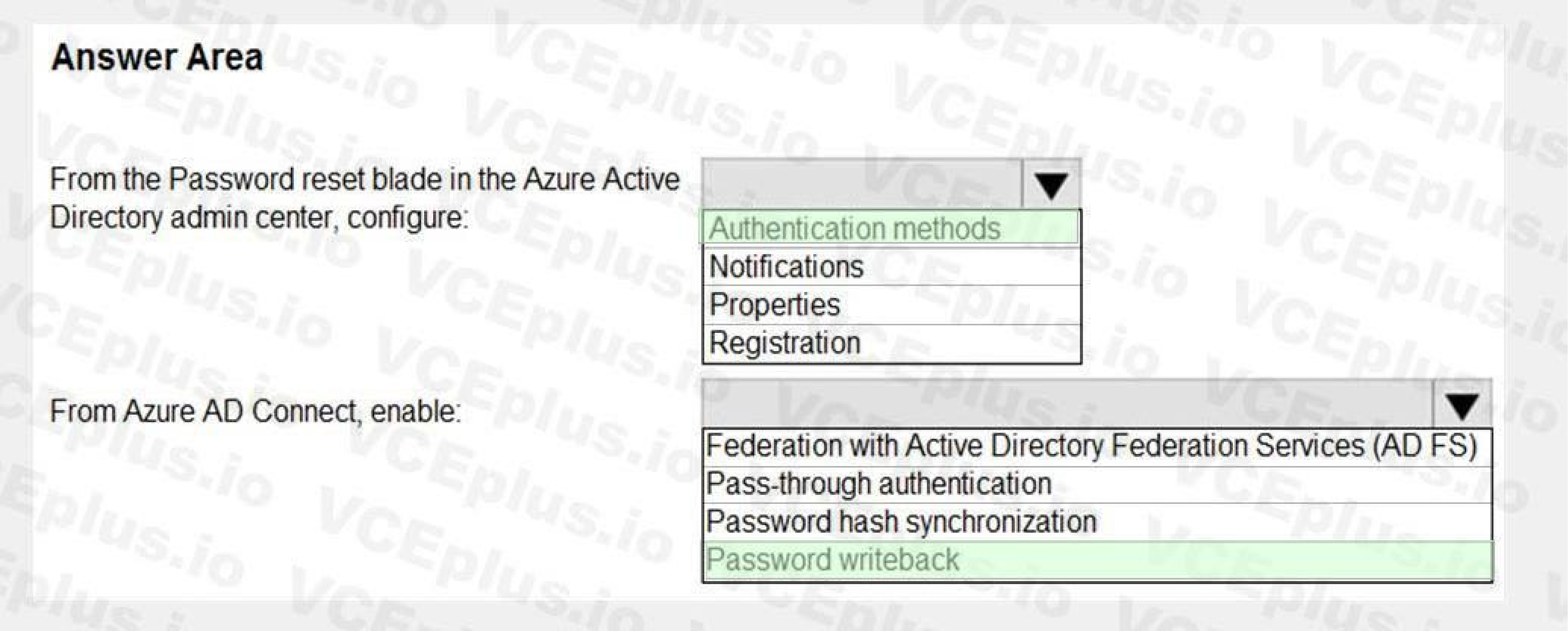
From the Password reset blade in the Azure Active Directory admin center, configure:

Authentication methods
Notifications
Properties
Registration

From Azure AD Connect, enable:

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

Answer Area:



Answer Area

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

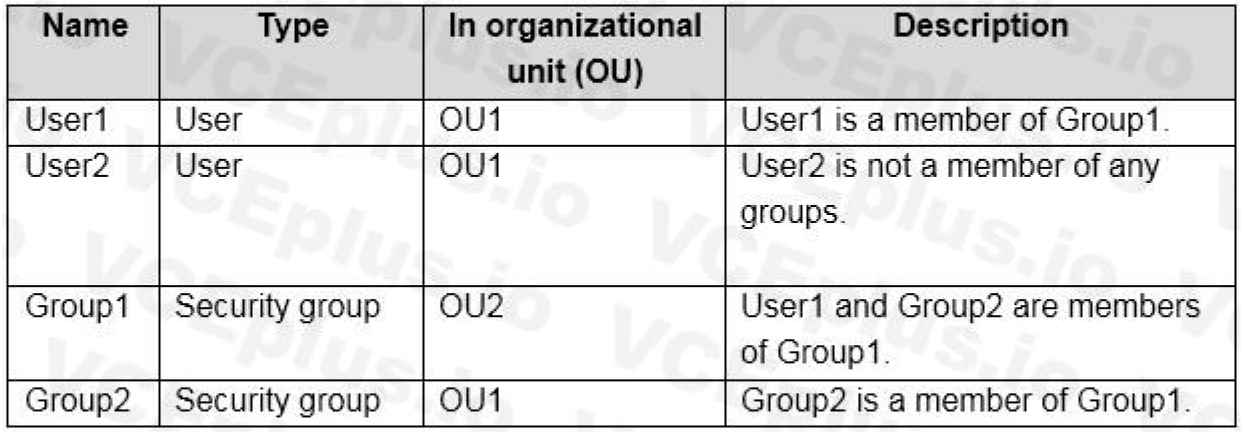
[✓ Authentication methods]
Notifications
Properties
Registration

From Azure AD Connect, enable:

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

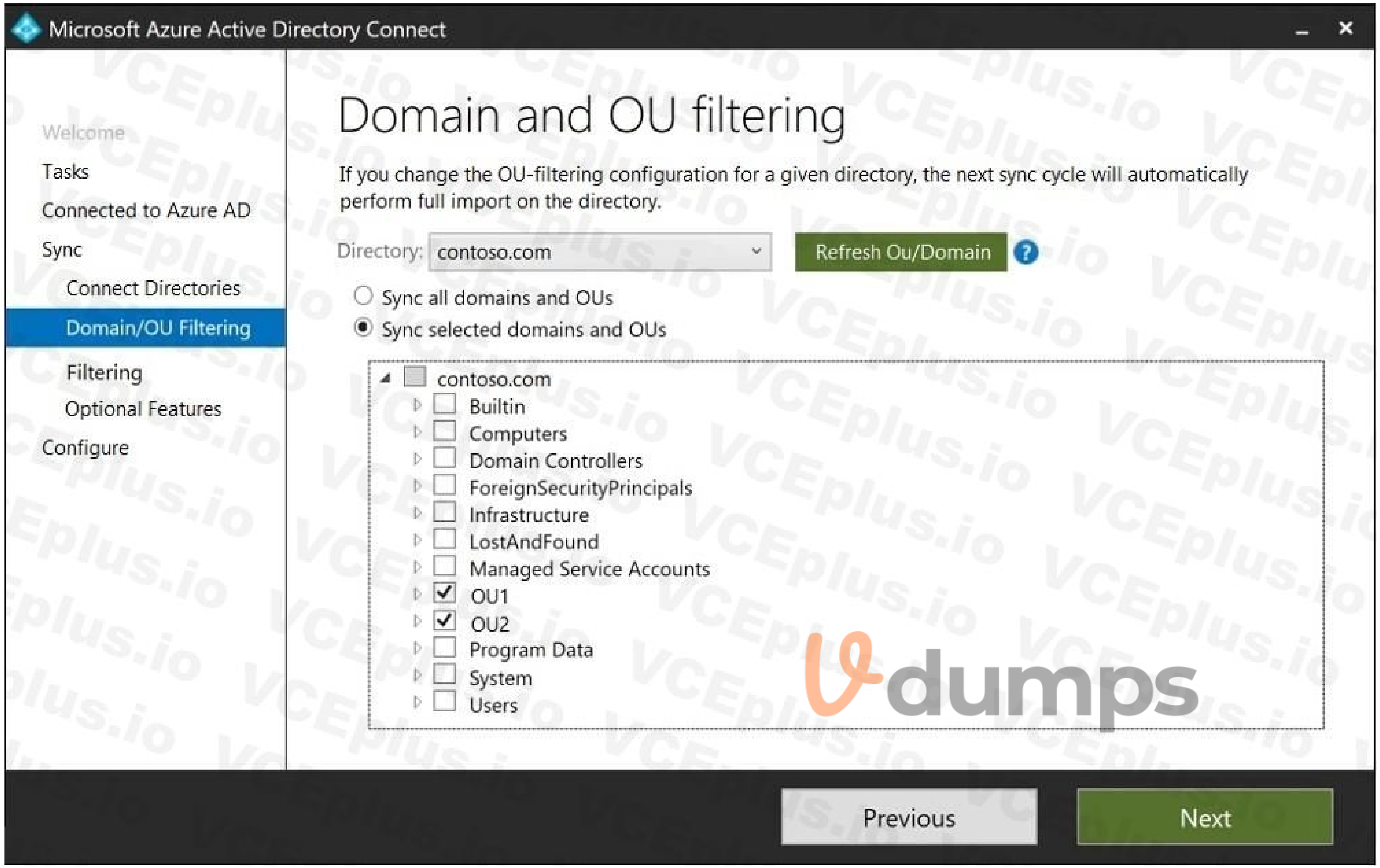
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-security-questions

QUESTION 35
HOTSPOT
Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the objects shown in the following table.



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

You install Azure AD Connect. You configure the Domain and OU filtering settings as shown in the Domain and OU Filtering exhibit. (Click the Domain and OU Filtering tab.)



Domain and OU filtering

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

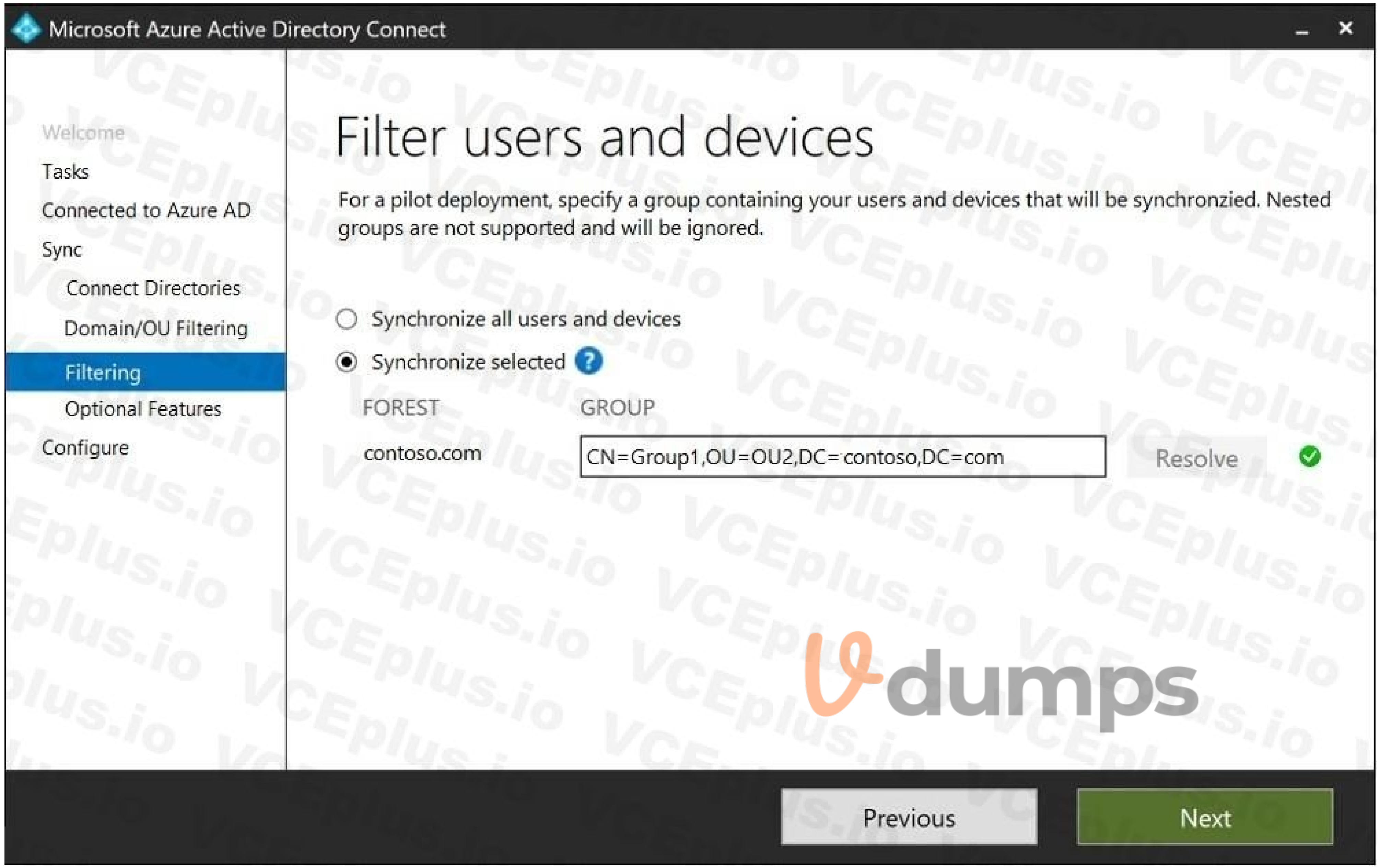
Directory: contoso.com

○ Sync all domains and OUs

● Sync selected domains and OUs

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

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



Filter users and devices

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

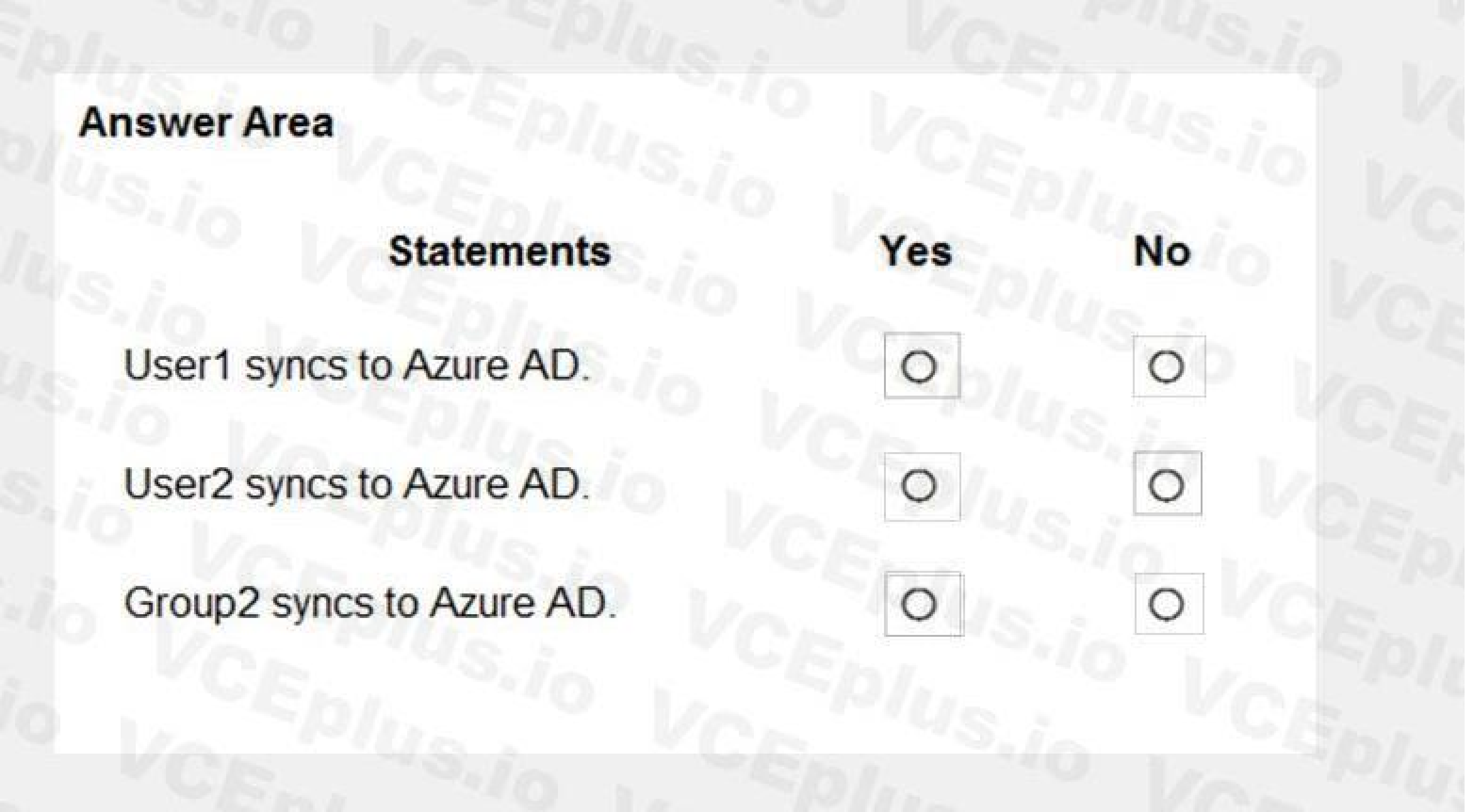
○ Synchronize all users and devices

● Synchronize selected

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

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

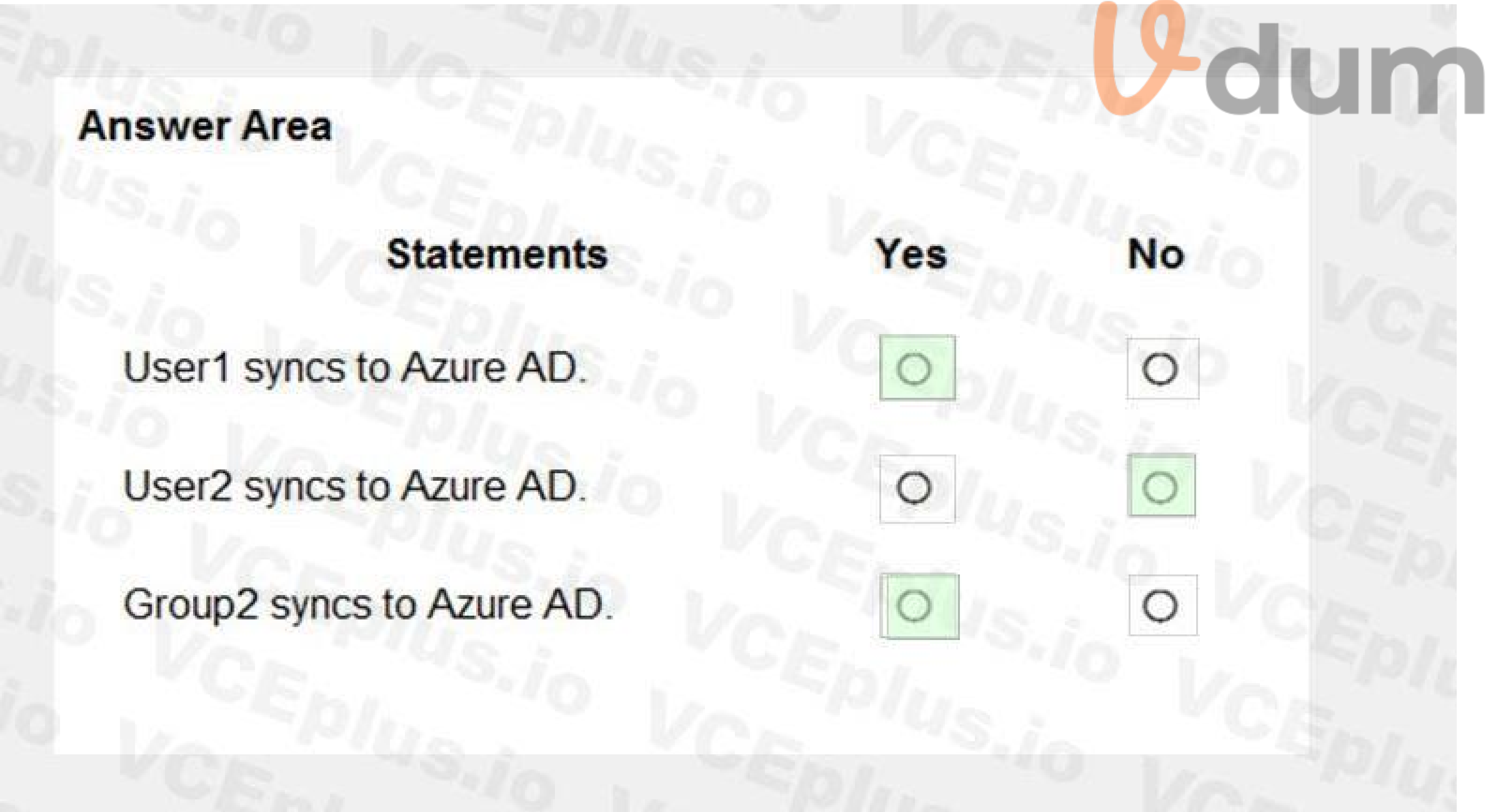
Hot Area:



Answer Area

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

Answer Area:



Answer Area

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

Section:

Explanation:

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

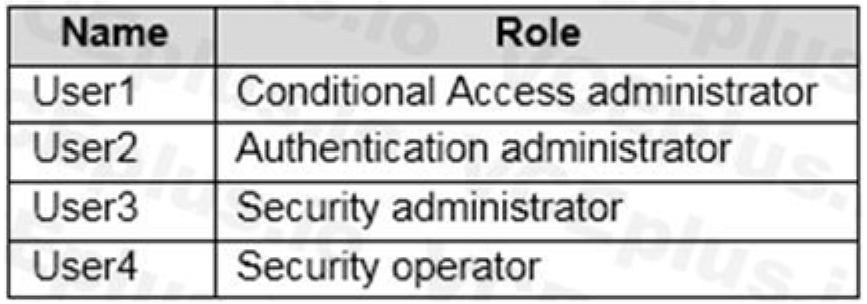
Reference:

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

QUESTION 36

HOTSPOT

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



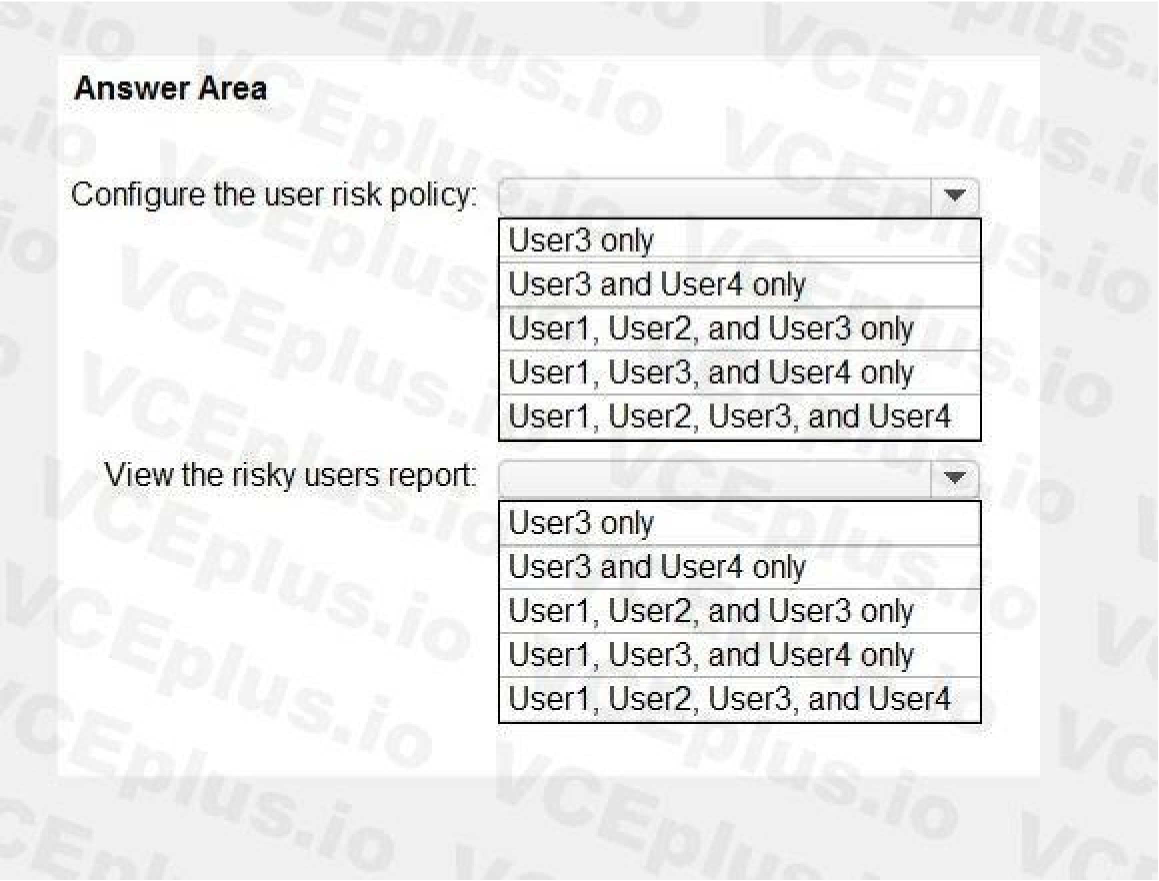
Name	Role
User1	Conditional Access administrator
User2	Authentication administrator
User3	Security administrator
User4	Security operator

You plan to implement Azure AD Identity Protection.

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

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

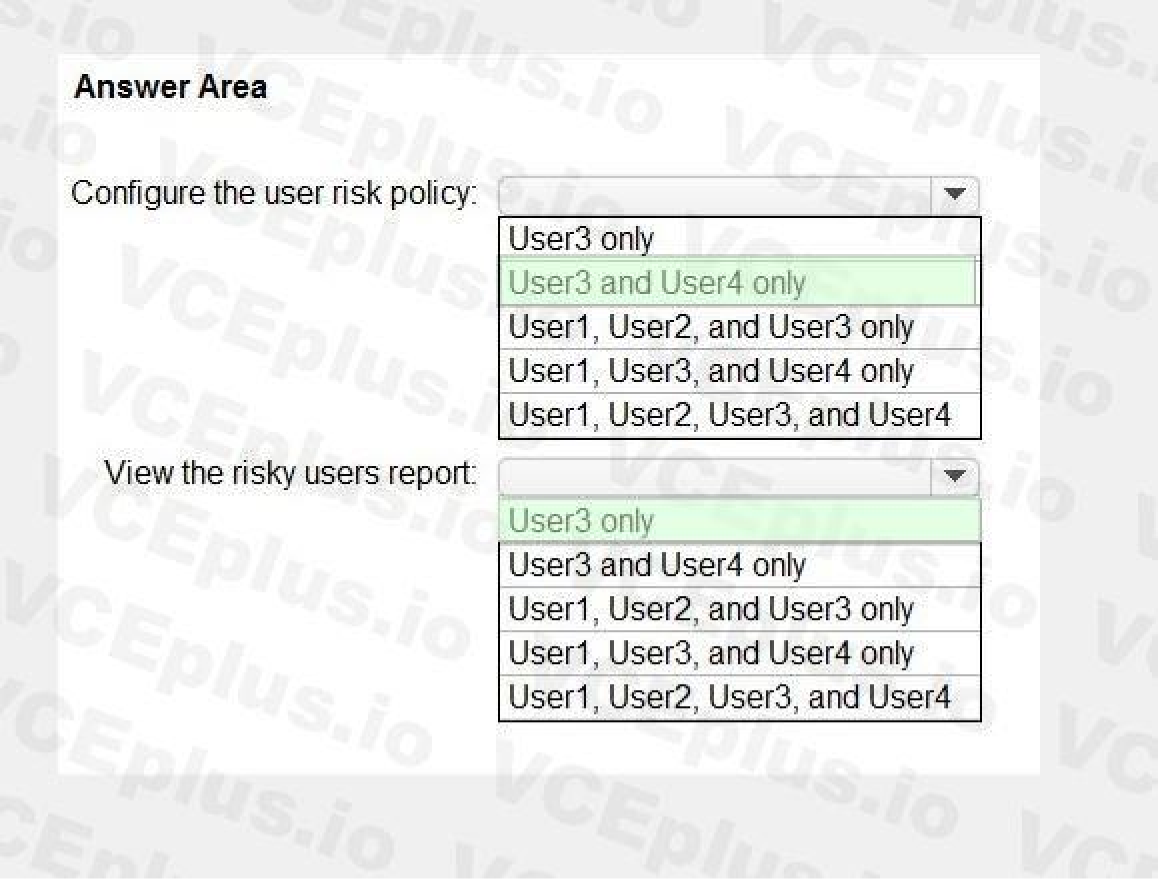
Configure the user risk policy:

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

View the risky users report:

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

Answer Area:



Answer Area

Configure the user risk policy:

- User3 only
- [✓ User3 and User4 only]
- User1, User2, and User3 only
- User1, User3, and User4 only
- User1, User2, User3, and User4

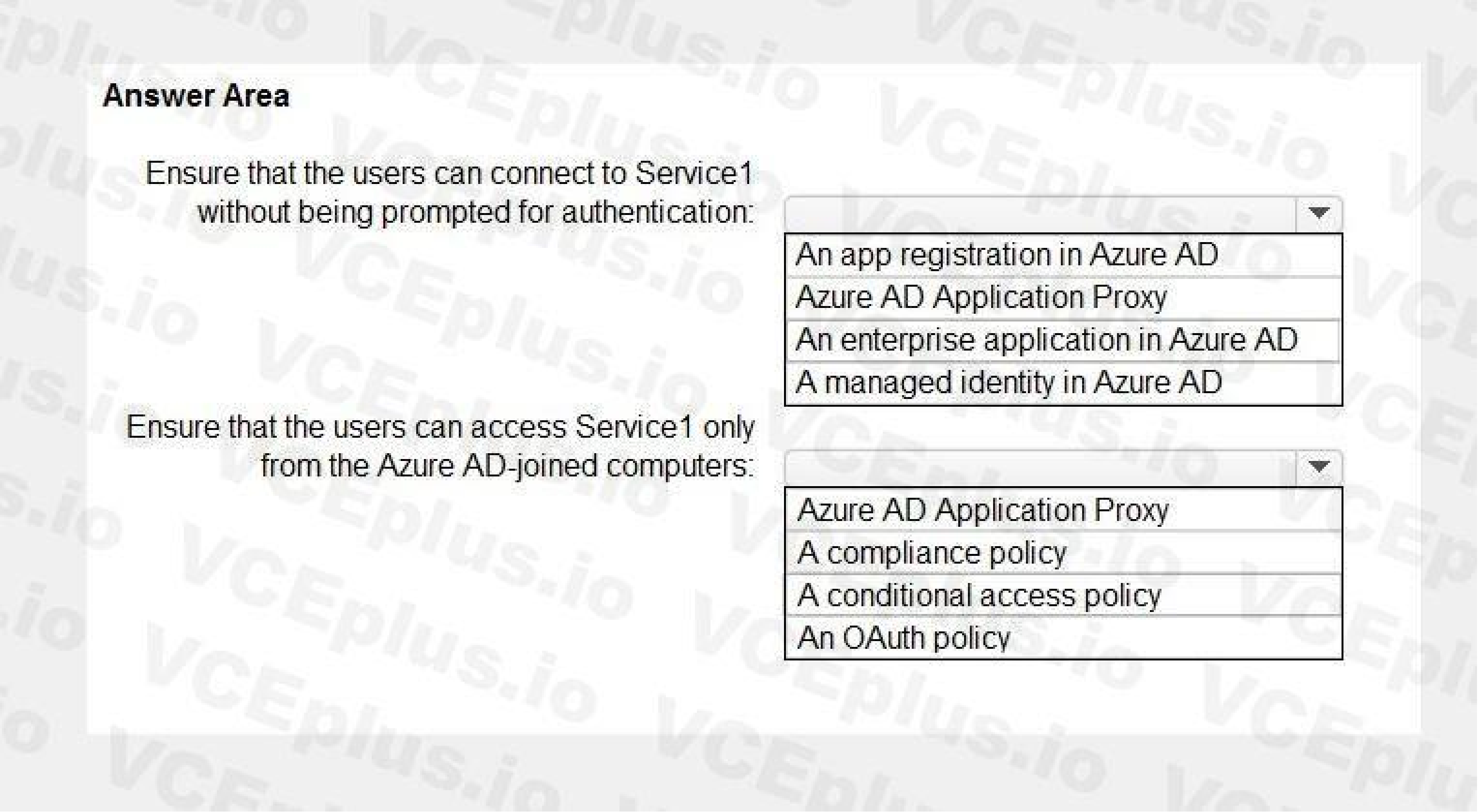
View the risky users report:

- [✓ User3 only]
- User3 and User4 only
- User1, User2, and User3 only
- User1, User3, and User4 only
- User1, User2, User3, and User4

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

QUESTION 37
HOTSPOT
Your company has a Microsoft 365 tenant.
All users have computers that run Windows 10 and are joined to the Azure Active Directory (Azure AD) tenant.
The company subscribes to a third-party cloud service named Service1. Service1 supports Azure AD authentication and authorization based on OAuth. Service1 is published to the Azure AD gallery.
You need to recommend a solution to ensure that the users can connect to Service1 without being prompted for authentication. The solution must ensure that the users can access Service1 only from Azure AD-joined computers. The solution must minimize administrative effort.
What should you recommend for each requirement? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

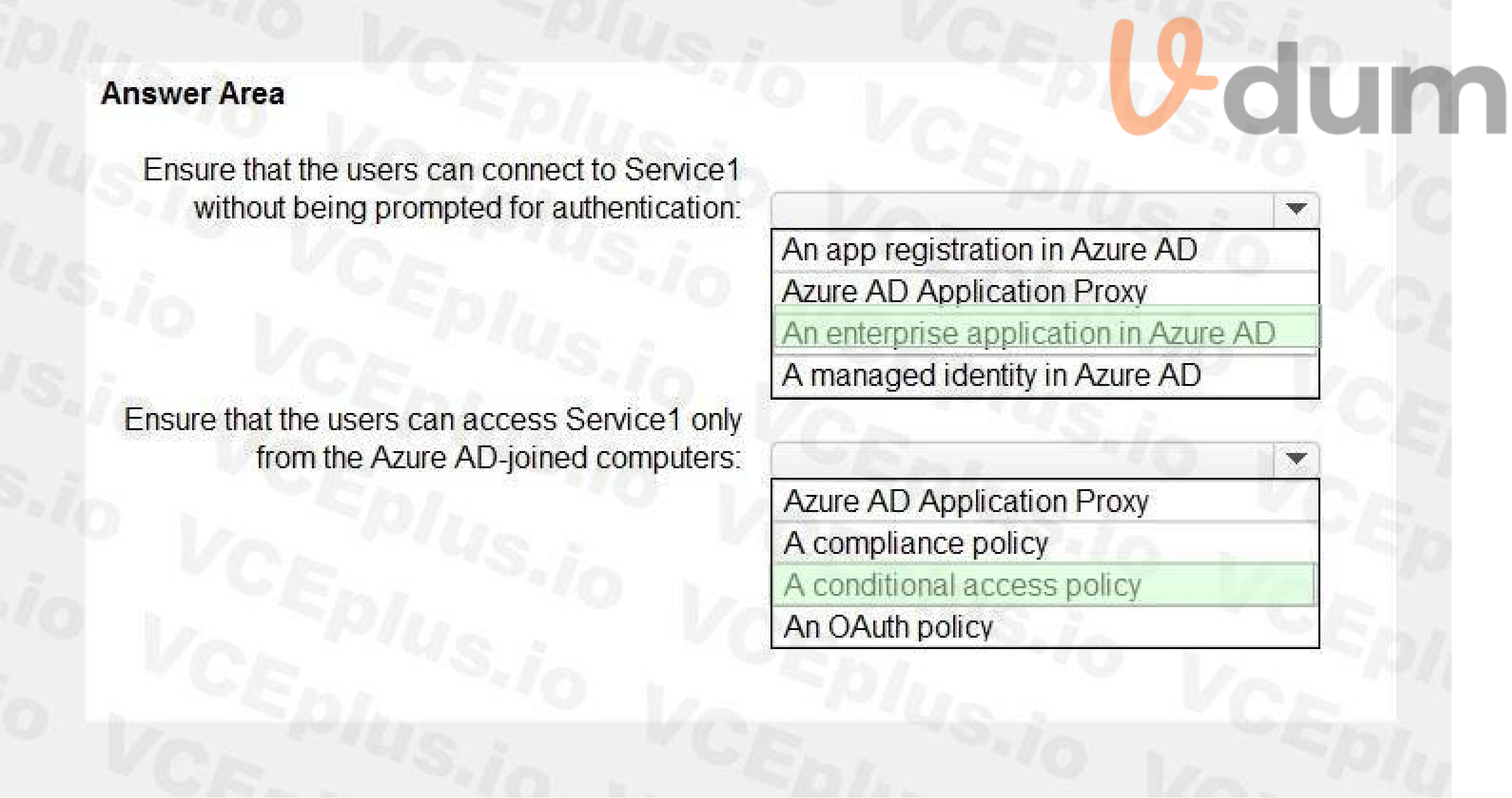
Ensure that the users can connect to Service1 without being prompted for authentication:

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

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

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

Answer Area:



Answer Area

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

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

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

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

Section:

Explanation:

Reference:

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

QUESTION 38

HOTSPOT

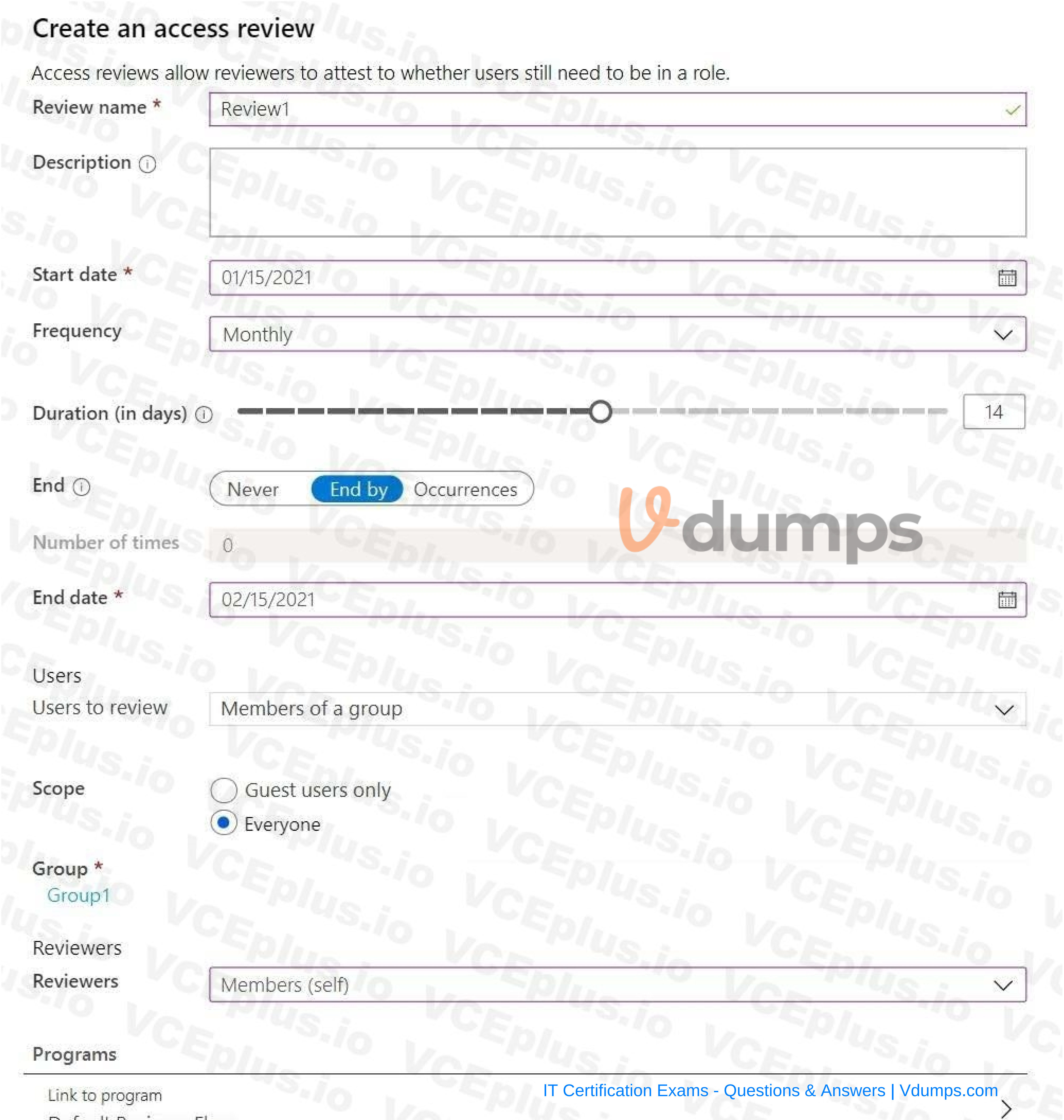
You have an Azure Active Directory (Azure AD) tenant that contains the following group:

Name: Group1

Members: User1, User2

Owner: User3

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



Create an access review

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

Review name * Review1 ✓

Description ⓘ

Start date * 01/15/2021

Frequency: Monthly

Duration (in days) ⓘ 14

End ⓘ Never [✓ End by] Occurrences

Number of times 0

End date * 02/15/2021

Users

Users to review: Members of a group

Scope

○ Guest users only

● Everyone

Group *

Group1

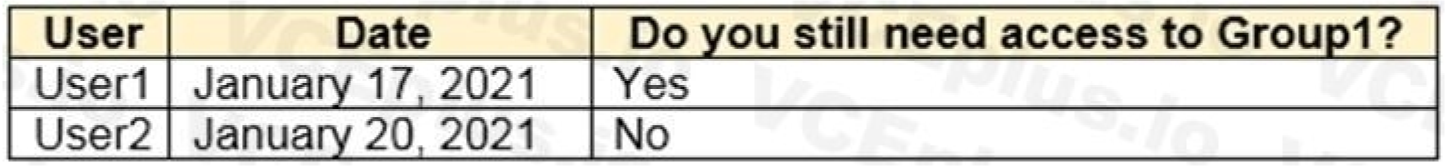
Reviewers

Reviewers: Members (self)

Programs

Link to program

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

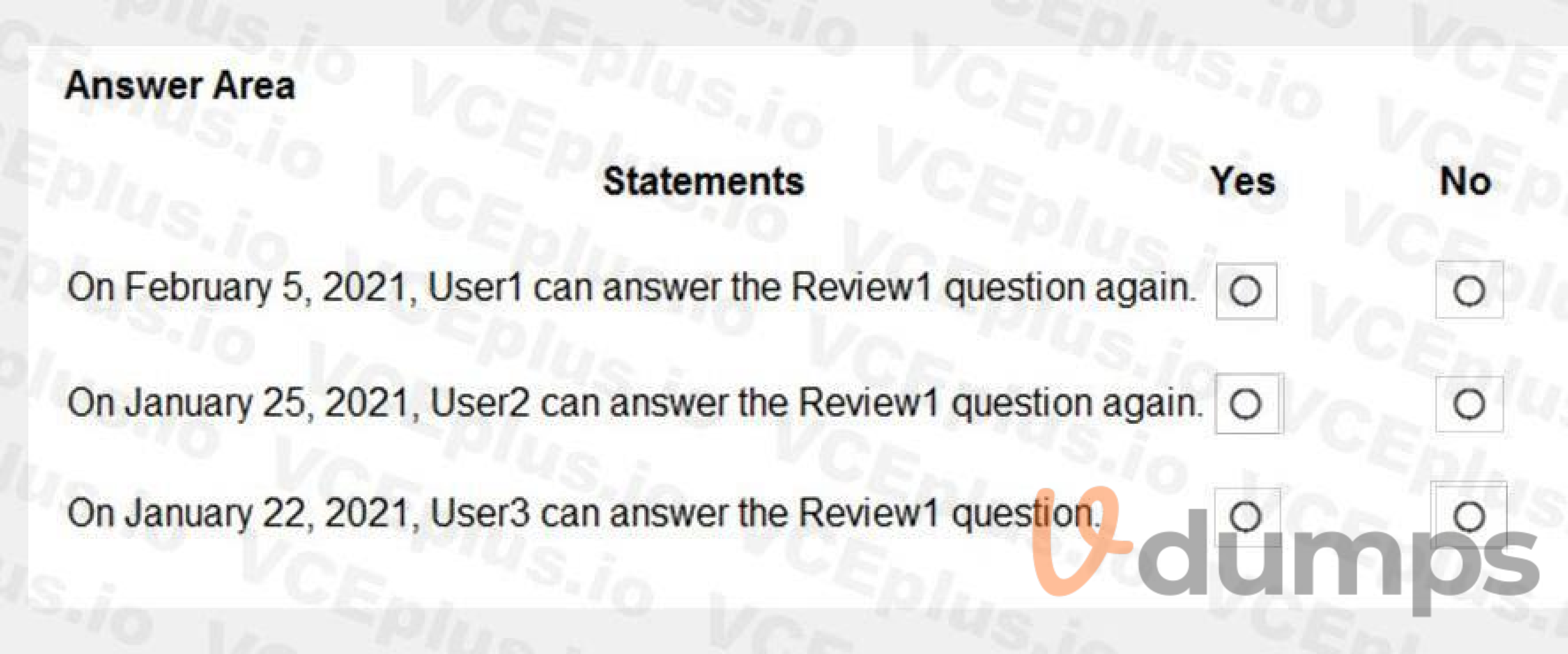


User	Date	Do you still need access to Group1?
User1	January 17, 2021	Yes
User2	January 20, 2021	No

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

NOTE: Each correct selection is worth one point.

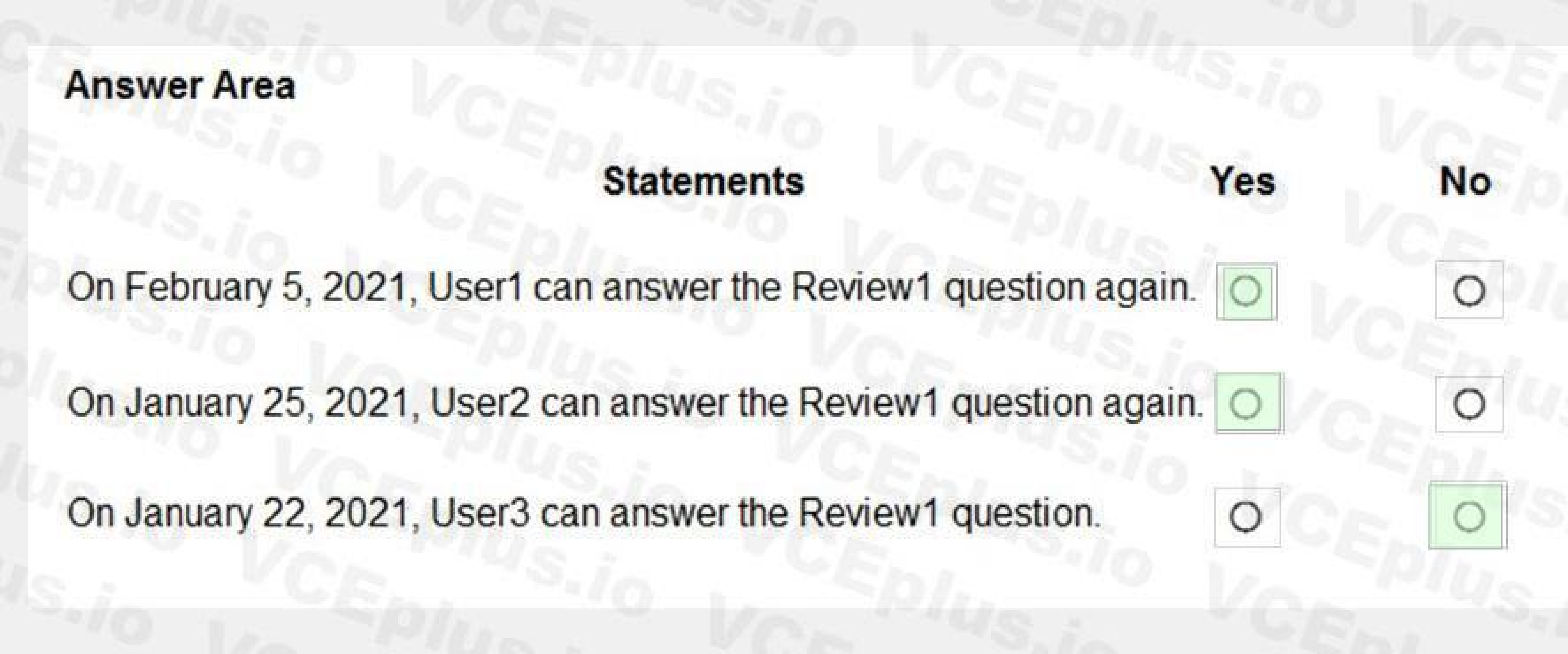
Hot Area:



Answer Area

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

Answer Area:



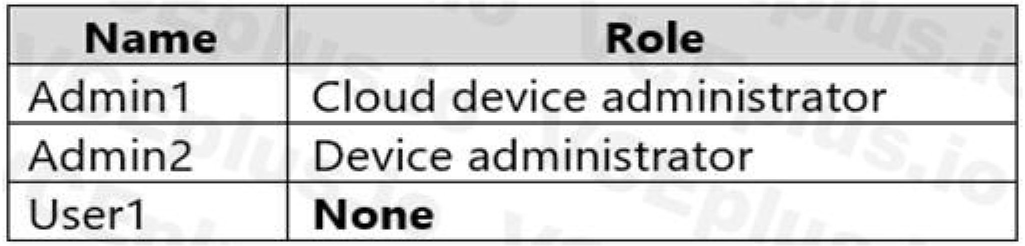
Answer Area

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

Section:

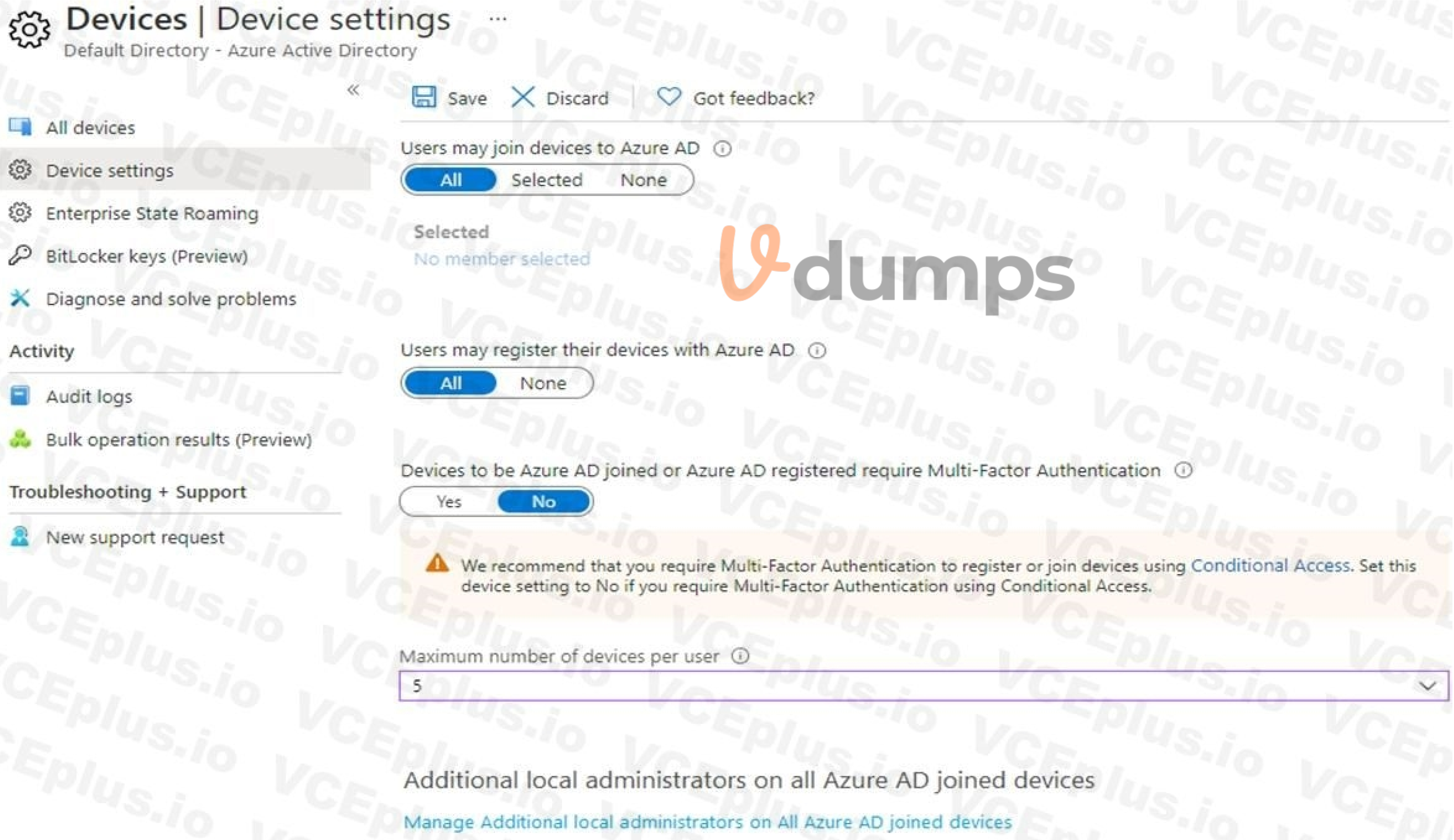
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/governance/review-your-access

QUESTION 39
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

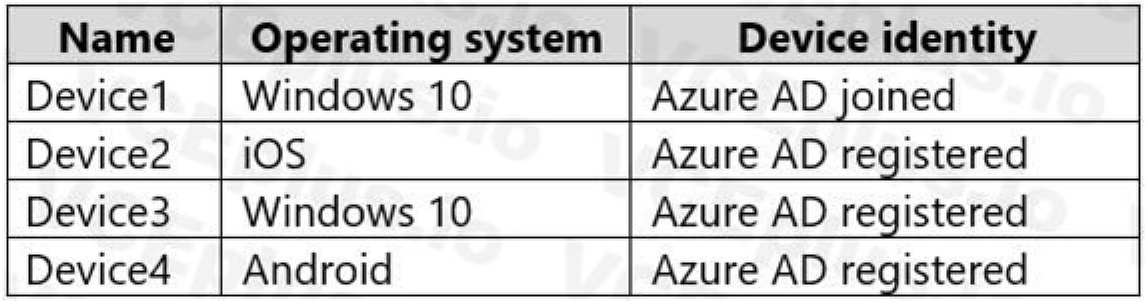
Devices to be Azure AD joined or Azure AD registered require Multi-Factor Authentication ⓘ
○ Yes ● No

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

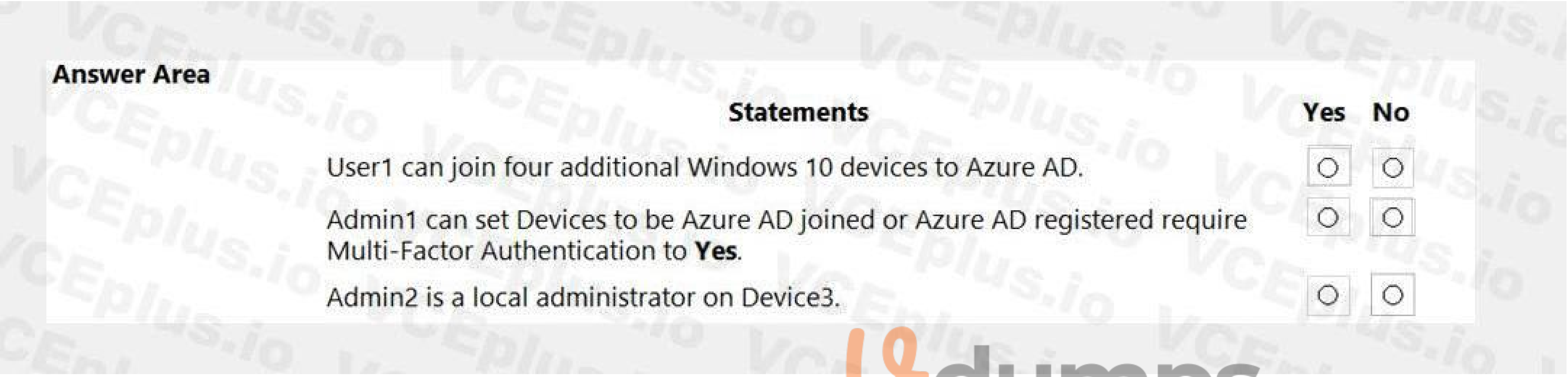
User1 has the devices shown in the following table.



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.

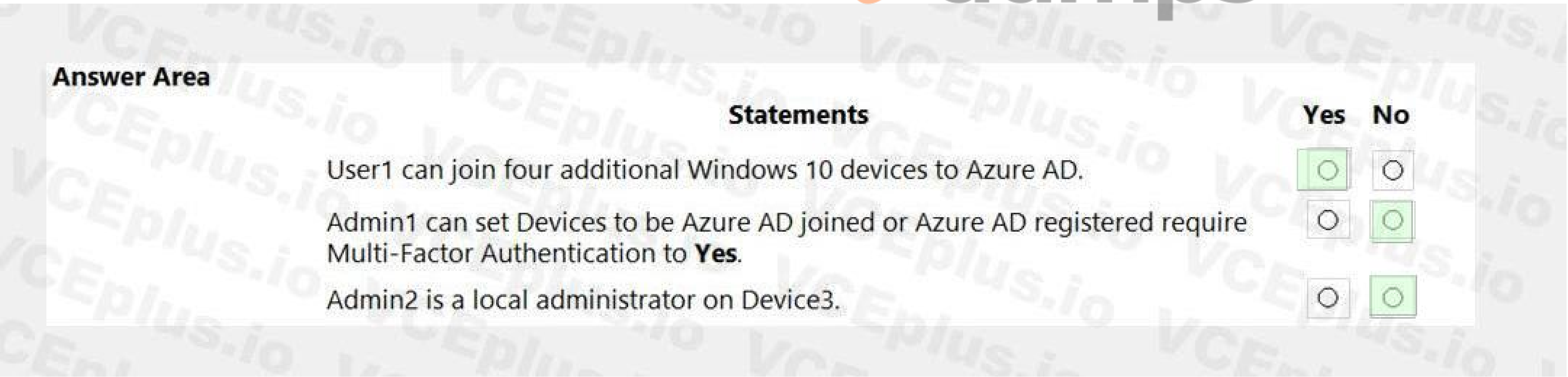
Hot Area:



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.	○	[✓ ○]

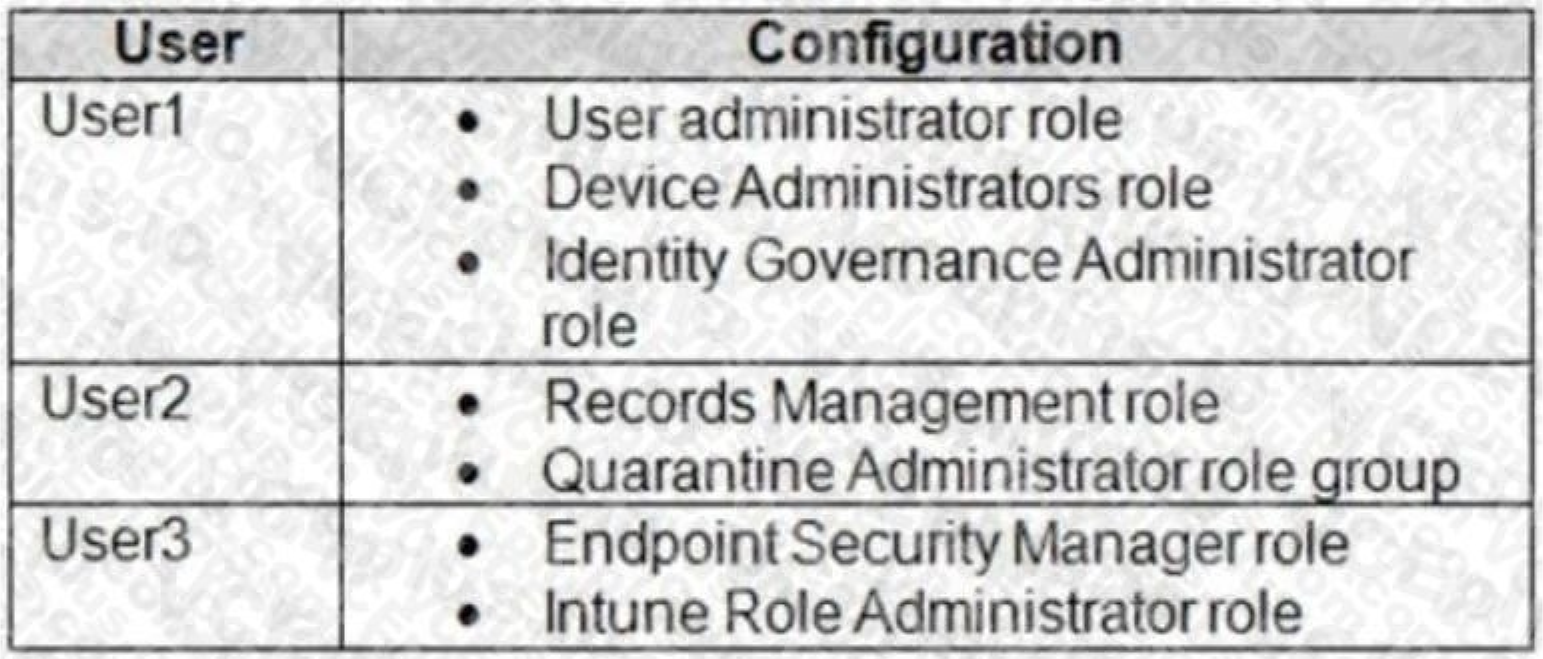
Section:
Explanation:
Box 1: Yes
Users may join 5 devices to Azure AD.
Box 2: No
Cloud device administrator an enable, disable, and delete devices in Azure AD and read Windows 10 BitLocker keys in the Azure portal. The role does not grant permissions to manage any other properties on the device.
Box 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 40

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.

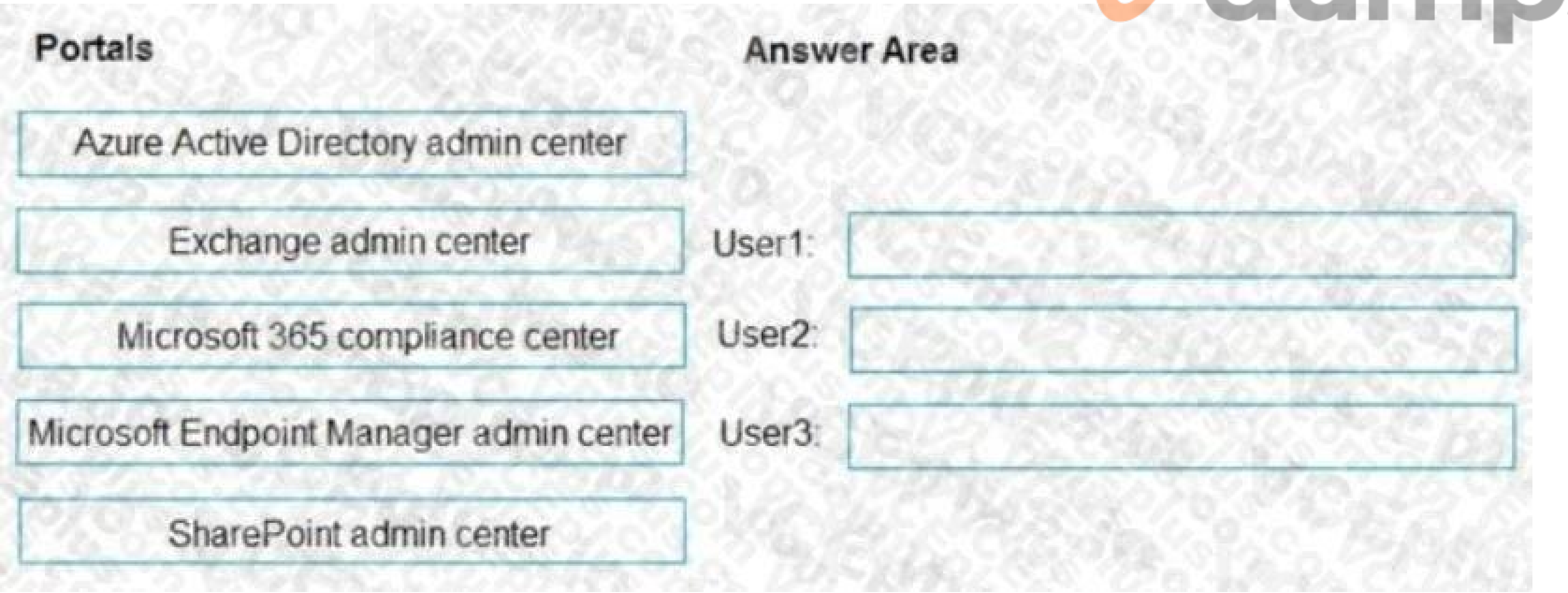


User	Configuration
User1	- User administrator role - Device Administrators role - Identity Governance Administrator role
User2	- Records Management role - Quarantine Administrator role group
User3	- Endpoint Security Manager role - Intune Role Administrator role

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

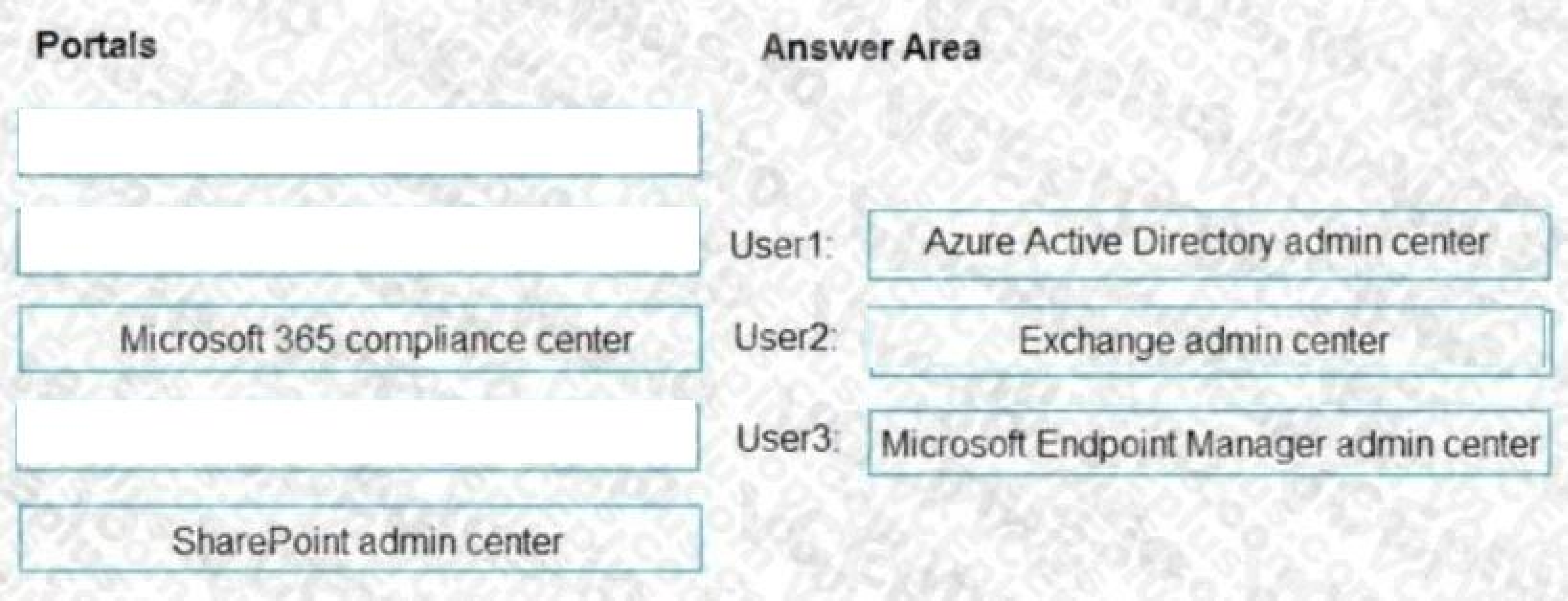
Answer Area

User1:

User2:

User3:

Correct Answer:



Portals		Answer Area
	User1:	Azure Active Directory admin center
Microsoft 365 compliance center	User2:	Exchange admin center
	User3:	Microsoft Endpoint Manager admin center
SharePoint admin center		

Section:
Explanation:

QUESTION 41

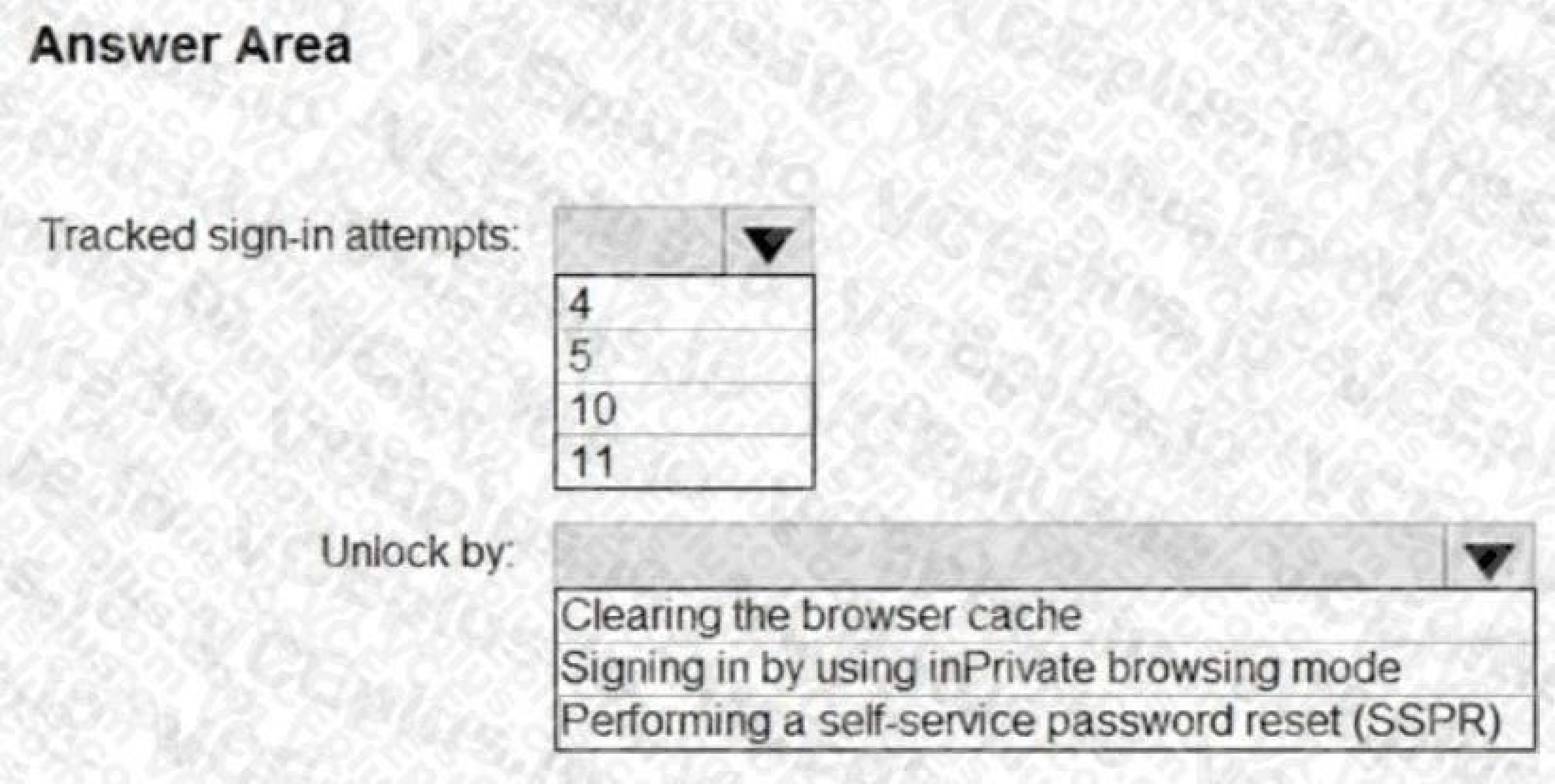
HOTSPOT

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

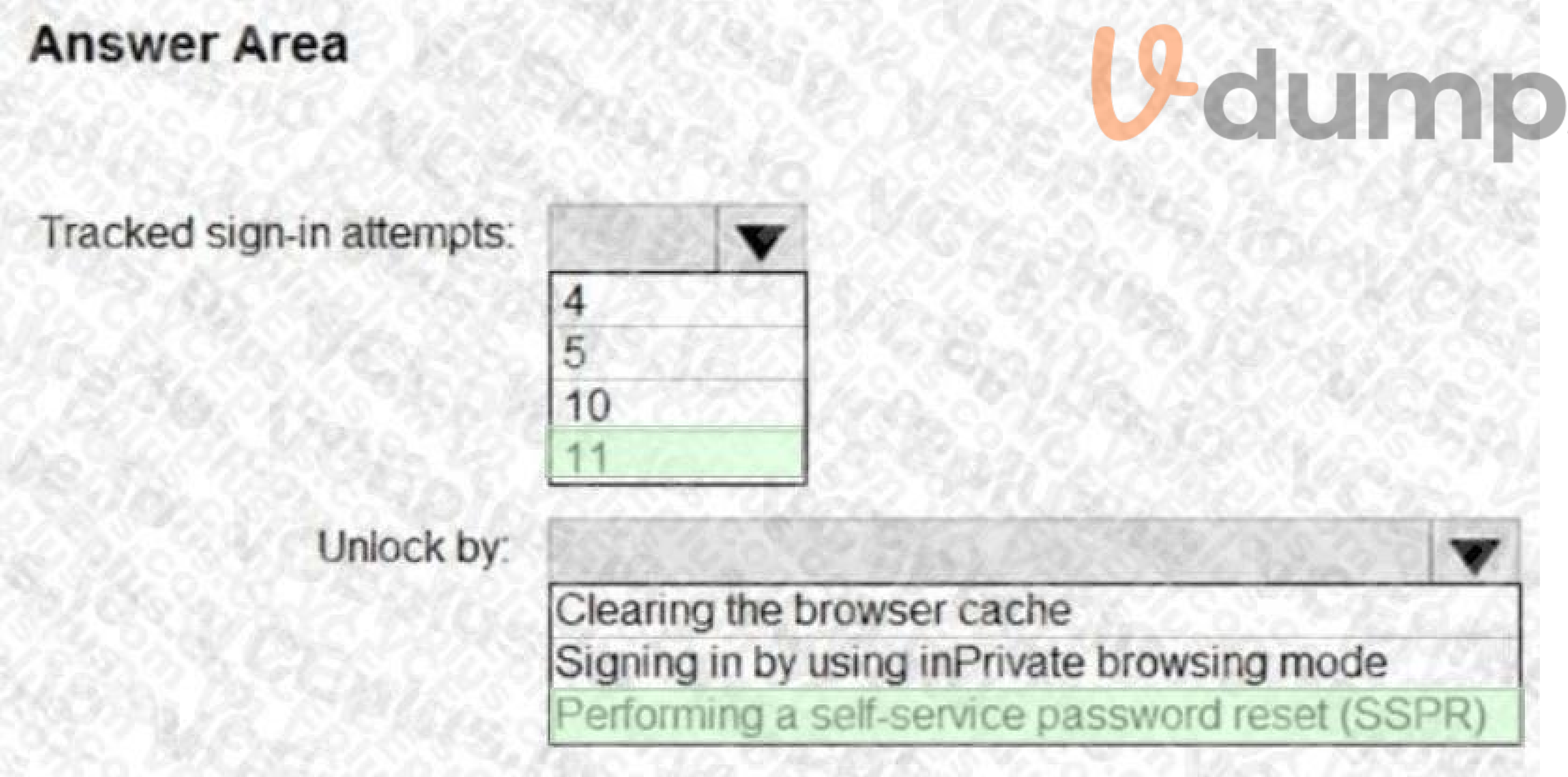
Tracked sign-in attempts:

- 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 42

HOTSPOT

You have an Azure subscription.

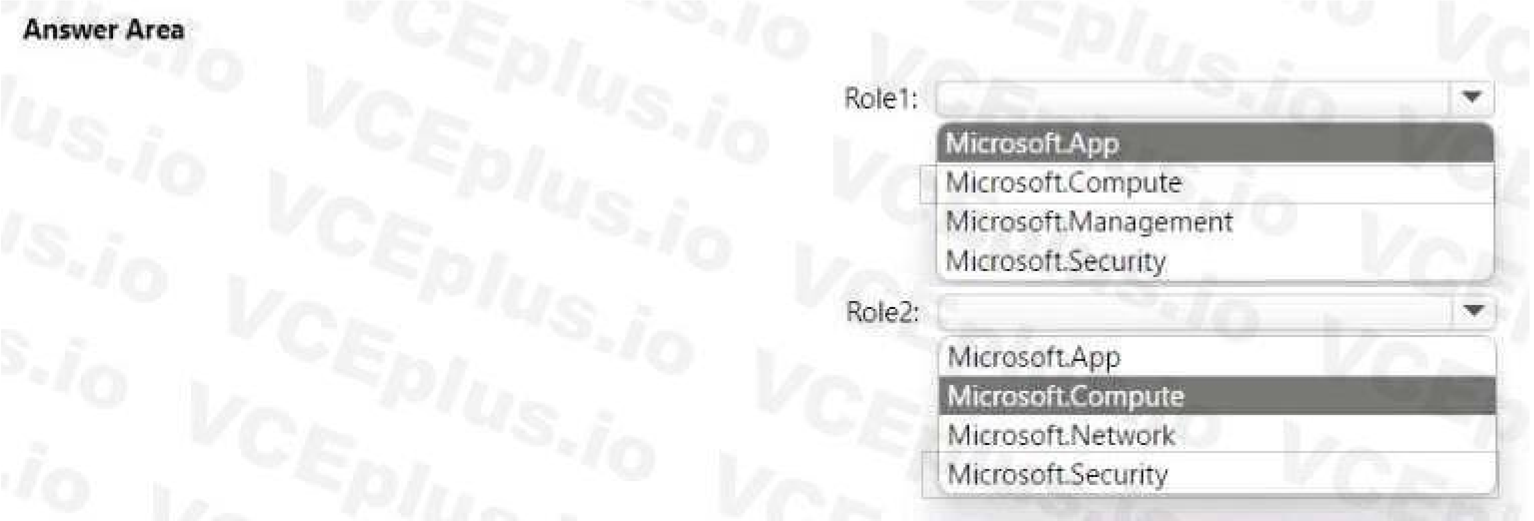
You need to create two custom roles named Role1 and Role2. The solution must meet the following requirements:

- 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:

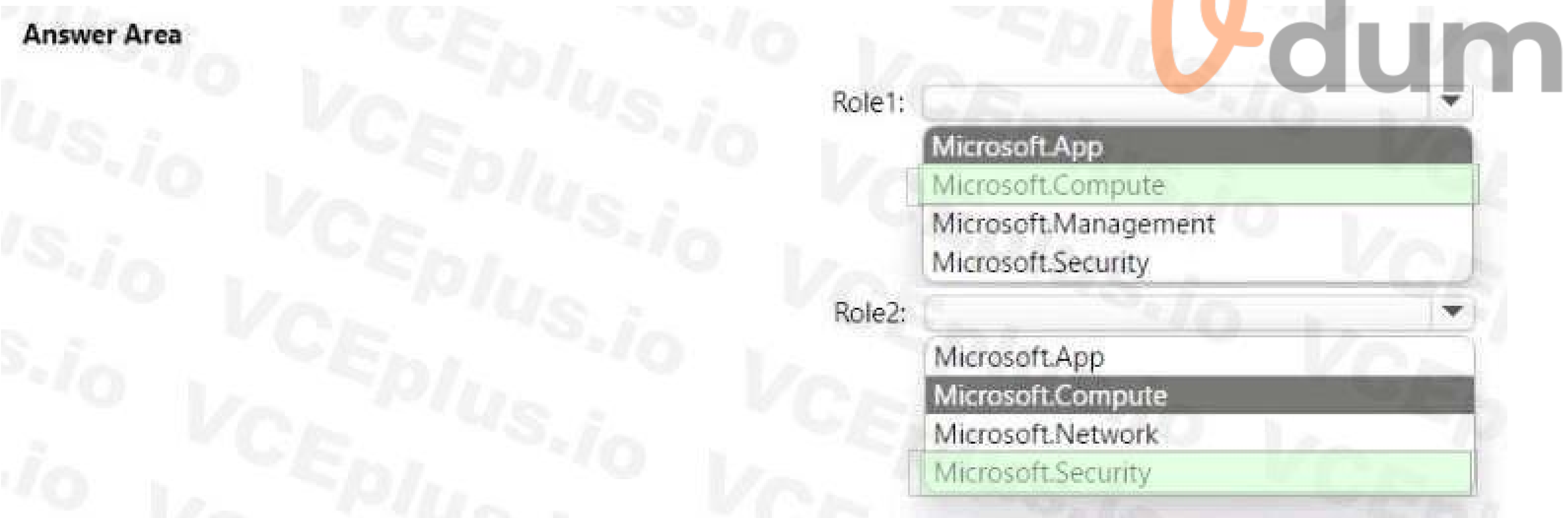


Answer Area

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 43

You have an Azure subscription that contains a user named User1. You need to meet the following requirements:

- Prevent User1 from being added as an owner of newly registered apps.
- Ensure that User1 can manage the application proxy settings.
- Ensure that User2 can register apps.
- Use the principle of least privilege.

Which role should you assign to User1?

A. Application developer

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

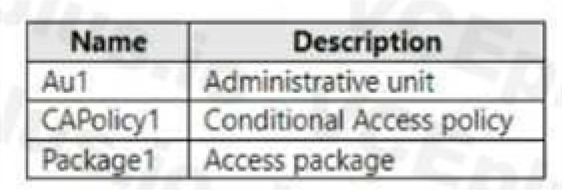
Correct Answer: D
Section:

QUESTION 44
Your company purchases 2 new Microsoft 365 ES subscription and an app named App.
You need to create a Microsoft Defender for Cloud Apps access policy for App1.
What should you do you first? (Choose Correct Answer based on Microsoft Identity and Access Administrator at microsoft.com)

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

Correct Answer: C
Section:
Explanation:
https://learn.microsoft.com/en-us/defender-cloud-apps/access-policy-aad
To create a Microsoft Defender for Cloud Apps access policy for App1, you should configure a Conditional Access policy to use app-enforced restrictions. This will allow you to control access to your cloud apps based on conditions such as user, device, location, and app state. You can also use app-enforced restrictions to control access to your cloud apps based on the state of the app, such as whether it's running on a managed or unmanaged device.

QUESTION 45
You have an Azure AD tenant named contoso.com that contains the resources shown in the following table.
You create a user named Admin 1.



Name	Description
Au1	Administrative unit
CAPolicy1	Conditional Access policy
Package1	Access package

You need to ensure that Admin can enable Security defaults for contoso.com.
What should you do first?

A. Configure Identity Governance.
B. Delete Package1.
C. Delete CAPolicy1.
D. Assign Admin1 the Authentication administrator role for Au1

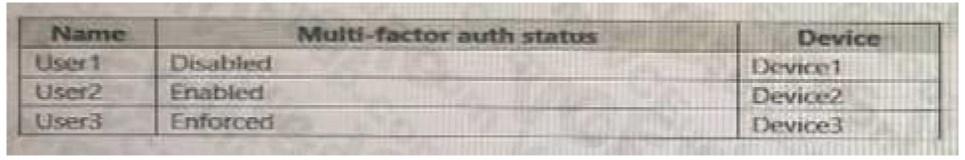
Correct Answer: D
Section:
Explanation:
To enable Security defaults for contoso.com, you should first sign in to the Azure portal as a security administrator, Conditional Access administrator, or global administrator. Then, browse to Azure Active Directory > Properties and select Manage security defaults. Set the Enable security defaults toggle to Yes and select Save.
After that, you can assign Admin1 the Identity Administrator role for Au1 to enable them to manage security defaults for the tenant.
https://practical365.com/what-are-azure-ad-security-defaults-and-should-you-use-them/

QUESTION 46
You have a Microsoft 365 tenant.
You currently allow email clients that use Basic authentication to conned to Microsoft Exchange Online.
You need to ensure that users can connect t to Exchange only run email clients that use Modern authentication protocols.
What should you implement?
You need to ensure that use Modern authentication

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

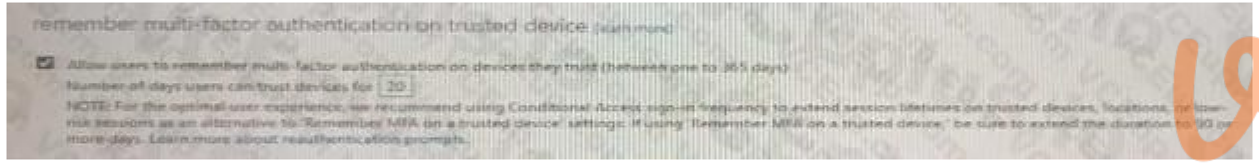
Correct Answer: C
Section:

QUESTION 47
You create the Azure Active Directory (Azure AD) users shown in the following table.



Name	Multi-factor auth status	Device
User1	Disabled	Device1
User2	Enabled	Device2
User3	Enforced	Device3

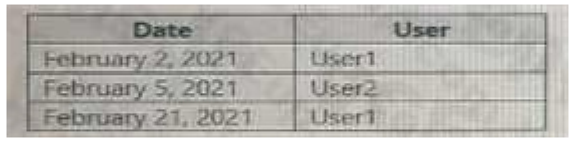
On February 1, 2021, you configure the multi-factor authentication (MFA) settings as shown in the following exhibit.



remember multi-factor authentication on trusted device (learn more)

☑ Allow users to remember multi-factor authentication on devices they trust (between one to 365 days)
Number of days users can trust devices for 20
NOTE: For the optimal user experience, we recommend using Conditional Access sign-in frequency to extend session lifetimes on trusted devices, locations, or low-risk sessions as an alternative to "Remember MFA on a trusted device" settings. If using "Remember MFA on a trusted device," be sure to extend the duration to 90 or more days. Learn more about reauthentication prompts.

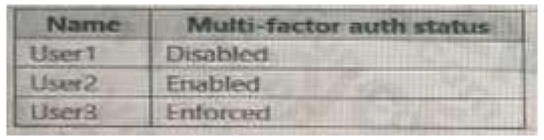
The users authentication to Azure AD on their devices as shown in the following table.



Date	User
February 2, 2021	User1
February 5, 2021	User2
February 21, 2021	User1

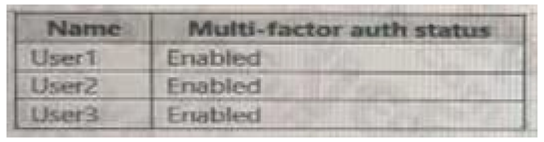
On February 26, 2021, what will the multi-factor auth status be for each user?

A.



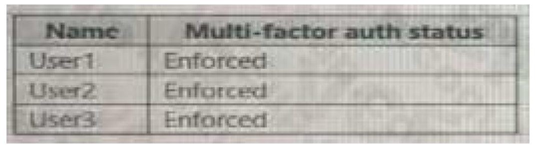
Name	Multi-factor auth status
User1	Disabled
User2	Enabled
User3	Enforced

B.



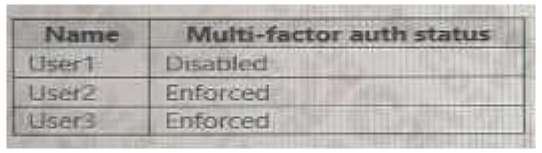
Name	Multi-factor auth status
User1	Enabled
User2	Enabled
User3	Enabled

C.



Name	Multi-factor auth status
User1	Enforced
User2	Enforced
User3	Enforced

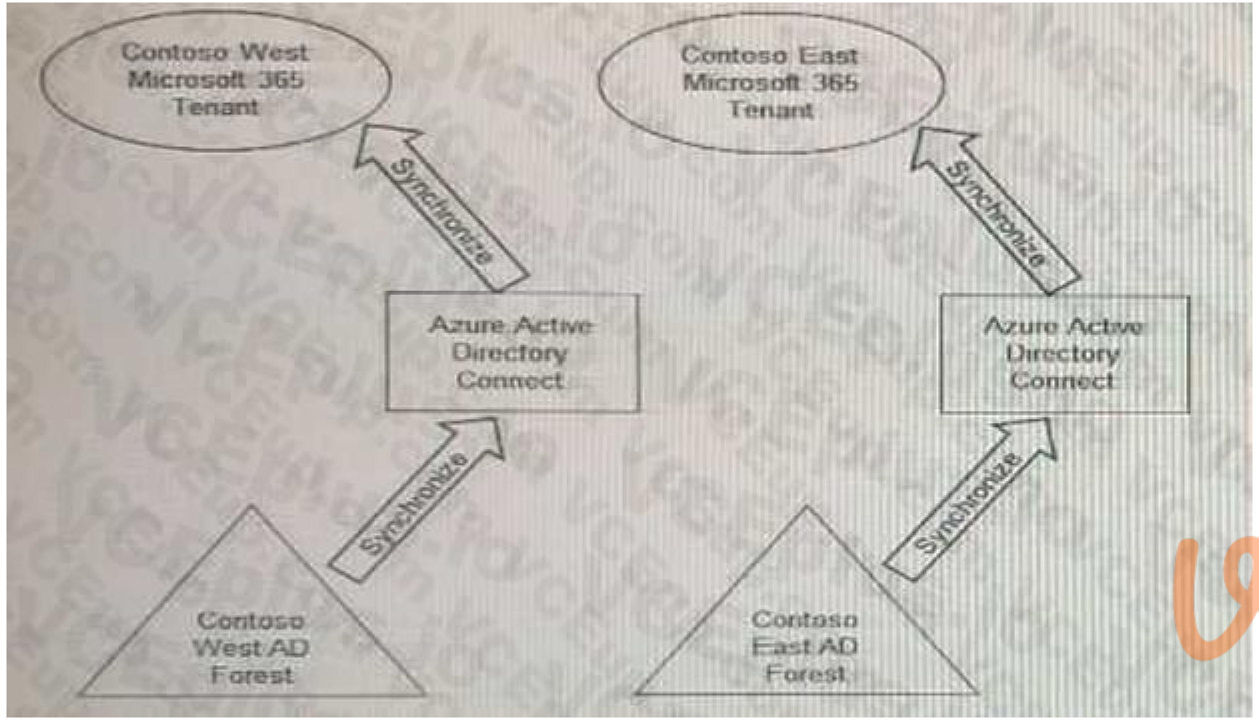
D.



Name	Multi-factor auth status
User1	Disabled
User2	Enforced
User3	Enforced

Correct Answer: B
Section:

QUESTION 48
Your company has two divisions named Contoso East and Contoso West. The Microsoft 365 identity architecture tor both divisions is shown in the following exhibit.

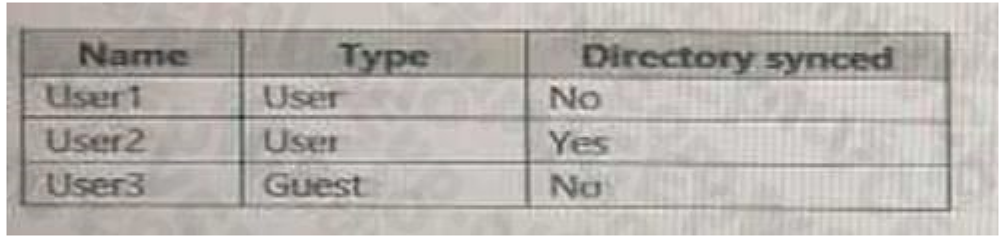

Contoso West Microsoft 365 Tenant
Contoso East Microsoft 365 Tenant
Synchronize
Synchronize
Azure Active Directory Connect
Azure Active Directory Connect
Synchronize
Synchronize
Contoso West AD Forest
Contoso East AD Forest

You need to assign users from the Contoso East division access to Microsoft SharePoint Online sites in the Contoso West tenant. The solution must not require additional Microsoft 3G5 licenses.
What should you do?

A. Configure The exiting Azure AD Connect server in Contoso Cast to sync the Contoso East Active Directory forest to the Contoso West tenant.
B. Configure Azure AD Application Proxy in the Contoso West tenant.
C. Deploy a second Azure AD Connect server to Contoso East and configure the server to sync the Contoso East Active Directory forest to the Contoso West tenant.
D. Invite the Contoso East users as guests in the Contoso West tenant.

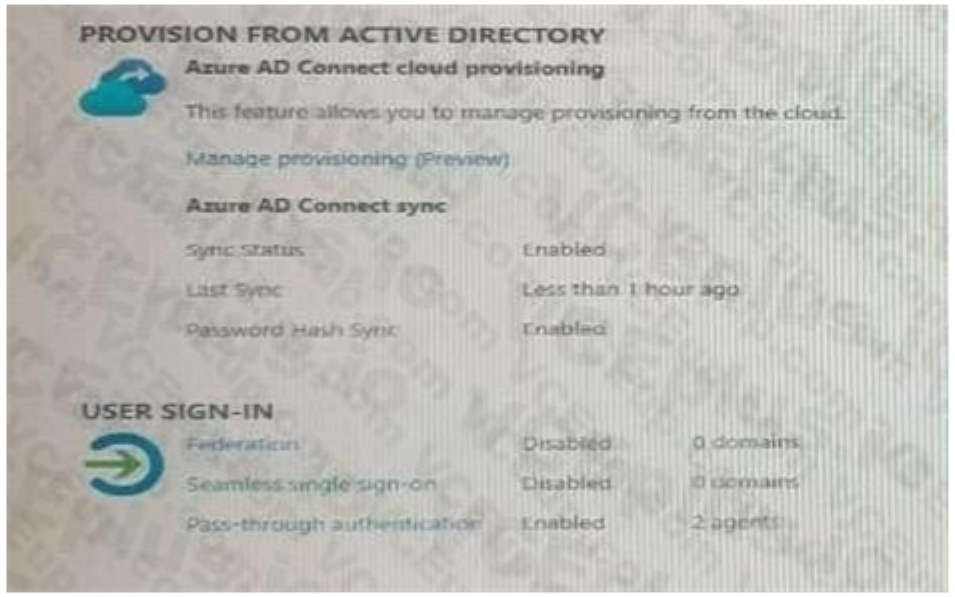
Correct Answer: D
Section:

QUESTION 49
Your network contains an on-premises Active Directory domain that sync to an Azure Active Directory (Azure AD) tenant. The tenant contains the shown in the following table.



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

All the users work remotely.
Azure AD Connect is configured in Azure as shown in the following exhibit.



PROVISION FROM ACTIVE DIRECTORY

Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

Manage provisioning (Preview)

Azure AD Connect sync

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

USER SIGN-IN

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

Connectivity from the on-premises domain to the internet is lost.
Which user can sign in to Azure AD?

A. User1 only
B. User1 and User 3 only
C. User1, and User2 only
D. User1, User2, and User3

Correct Answer: A
Section:

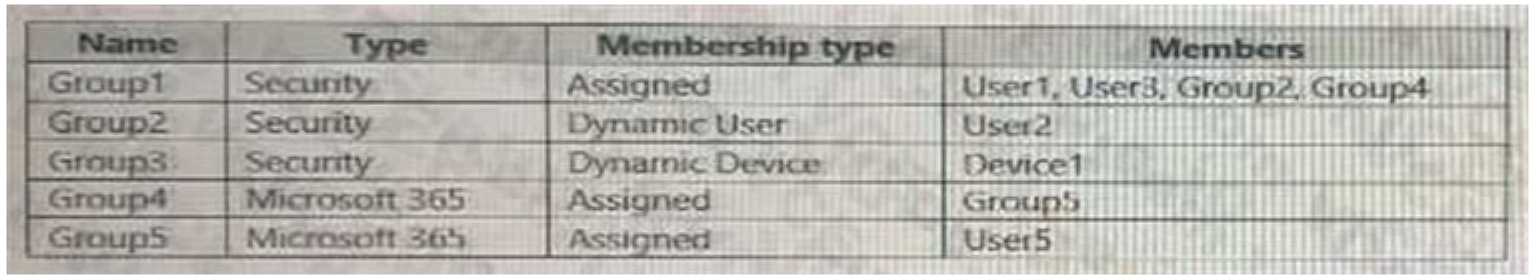
QUESTION 50
You have an Azure Active Directory (Azure AD) tenant named contoso.com.
You need to ensure that Azure AD External Identities pricing is based on monthly active users (MAU).
What should you configure?

A. an access review
B. the terms or use
C. a linked subscription
D. a user flow

Correct Answer: C
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/external-identitiespricing

QUESTION 51
You have an Azure Active Directory (Azure Azure) tenant that contains the objects shown in the following table.
- A device named Device1
- Users named User1, User2, User3, User4, and User5
- Five groups named Group1, Group2, Group3, Ciroup4, and Group5

The groups are configured as shown in the following table.



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

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

A. 0
B. 2
C. 3
D. 4

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

QUESTION 52
You have a Microsoft Exchange organization that uses an SMTP' address space of contoso.com.
Several users use their contoso.com email address for self-service sign up to Azure Active Directory (Azure AD).
You gain global administrator privileges to the Azure AD tenant that contains the self-signed users.
You need to prevent the users from creating user accounts in the contoso.com Azure AD tenant for self-service sign-up to Microsoft 365 services.
Which PowerShell cmdlet should you run?

A. Set-MsolCompanySettings
B. Set-MsolDomainFederationSettings
C. Update-MsolfederatedDomain
D. Set-MsolDomain

Correct Answer: A
Section:
Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/directory-self-servicesignup

QUESTION 53
Your network contains an on-premises Active Directory domain that syncs to an Azure Active Directory (Azure AD) tenant- Users sign in to computers that run Windows 10 and are joined to the domain.
You plan to implement Azure AD Seamless Single Sign-On (Azure AD Seamless SSO).
You need to configure the computers for Azure AD Seamless SSO.
What should you do?

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

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

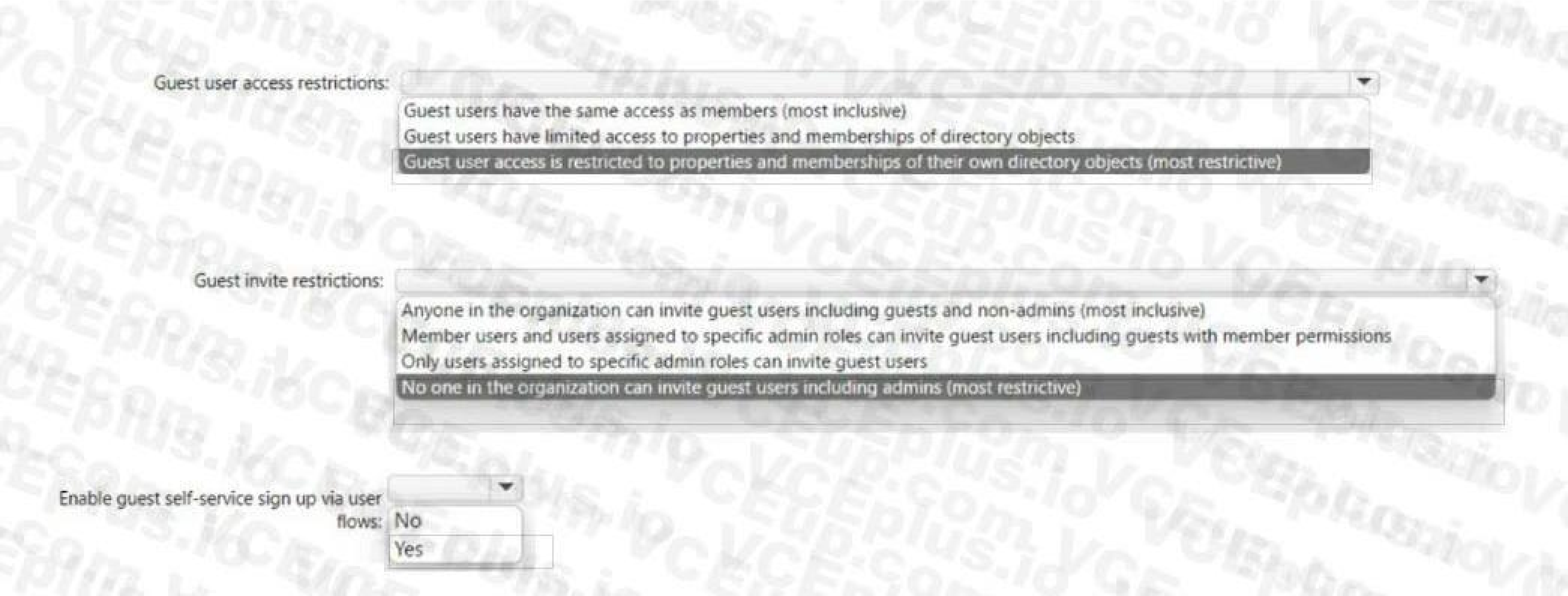
QUESTION 54
You use Azure Monitor to analyze Azure Active Directory (Azure AD) activity logs.
Yon receive more than 100 email alerts each day for tailed Azure Al) user sign-in attempts.
You need to ensure that a new security administrator receives the alerts instead of you.
Solution: From Azure AD, you create an assignment for the Insights at administrator role.
Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section:

QUESTION 55
HOTSPOT
You have an Azure AD tenant that contains a user named User1. User1 is assigned the User Administrator role.
You need to configure External collaboration settings for the tenant to meet the following requirements:
*Guest users must be prevented from querying staff email addresses.
*Guest users must be able to access the tenant only if they are invited by User1.
Which three settings should you configure? To answer, select the appropriate settings in the answer area.

Hot Area:

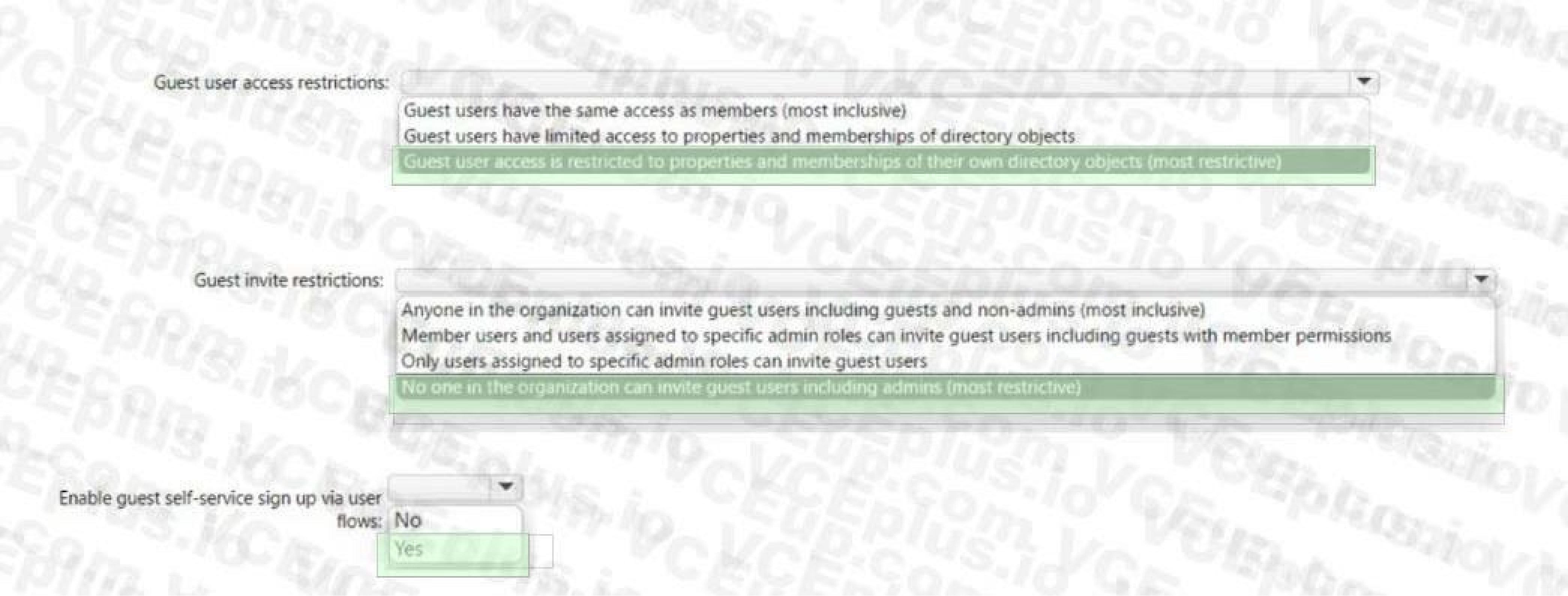


Guest user access restrictions:
- Guest users have the same access as members (most inclusive)
- Guest users have limited access to properties and memberships of directory objects
- Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

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

Enable guest self-service sign up via user flows:
- No
- Yes

Answer Area:



Guest user access restrictions:

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

Guest invite restrictions:

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

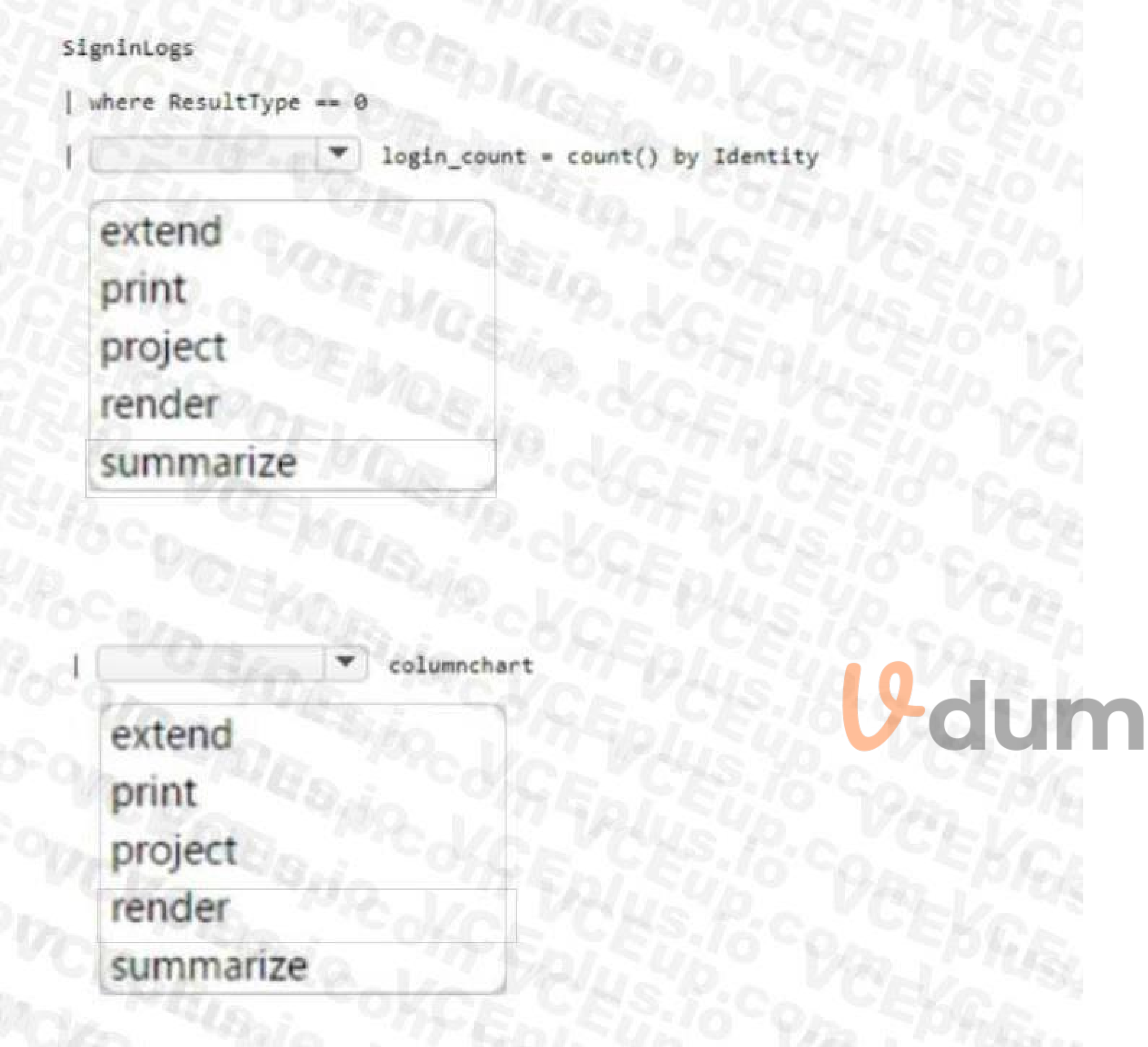
Enable guest self-service sign up via user flows:

- No
- [✓ Yes]

Section:
Explanation:
Box1 = User access is restricted to properties and memberships of their own directory objects (most restrictive). This setting ensures that guest users are prevented from querying staff email addresses and can access the tenant only if they are invited by User1.
Box2 = Only users assigned to specific admin roles can invite guest users. This setting ensures that guest users can access the tenant only if they are invited by User1.
Box3 = This setting enables guest users to sign up for the tenant only if they are invited by User1.

QUESTION 56
HOTSPOT
You have an Azure subscription.
Azure AD logs are sent to a Log Analytics workspace.
You need to query the logs and graphically display the number of sign-ins per user.
How should you complete the query? To answer, select the appropriate options in the answer area.

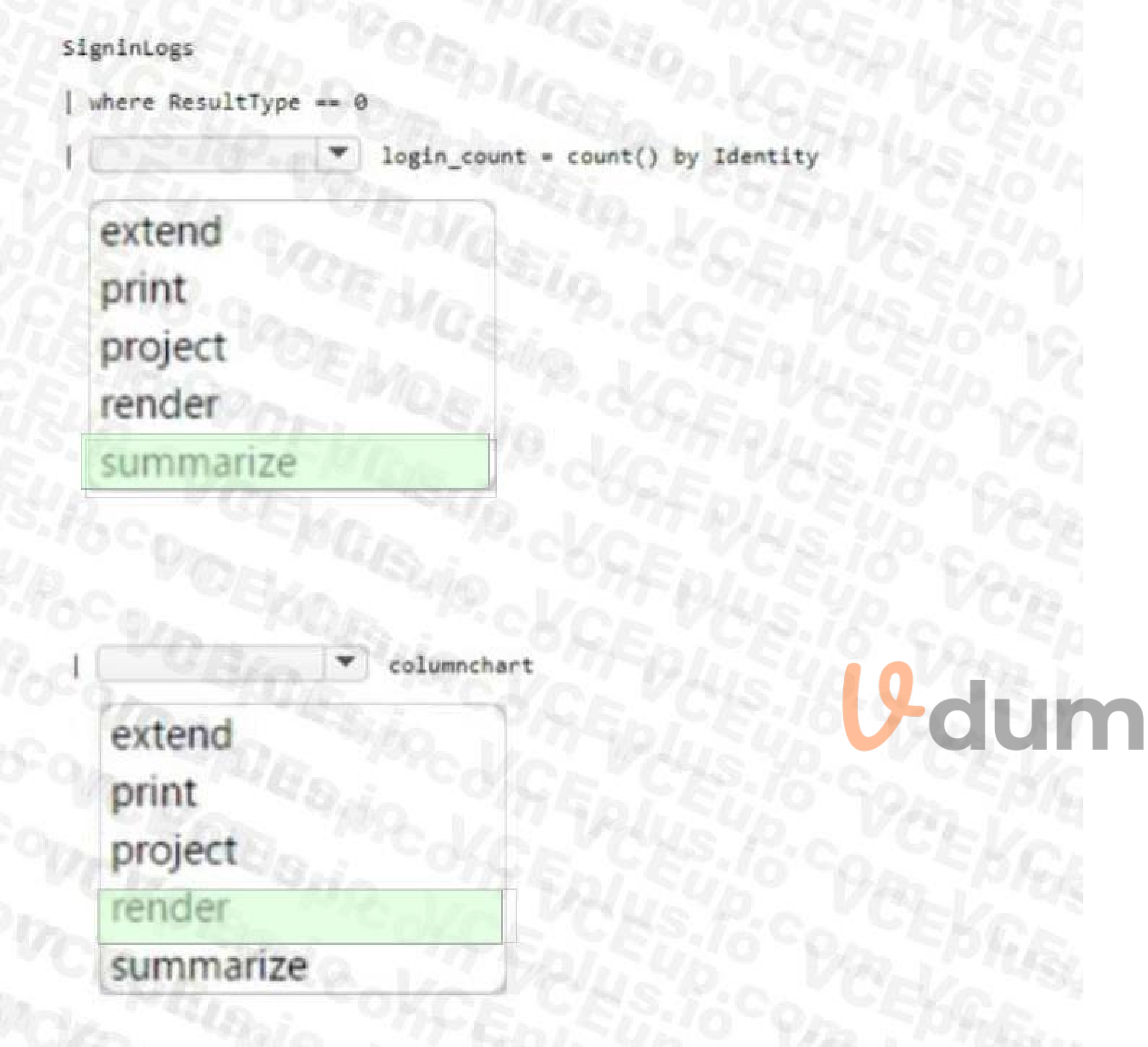
Hot Area:



```
SigninLogs
| where ResultType == 0
|                login_count = count() by Identity

|                columnchart
```

Answer Area:

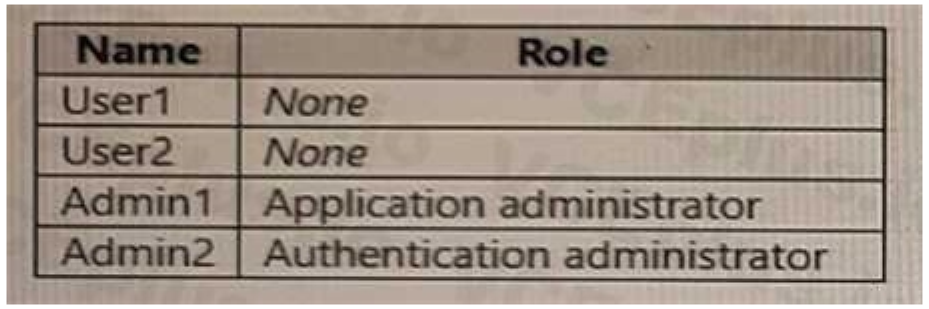


```
SigninLogs
| where ResultType == 0
|                      login_count = count() by Identity
```

```
|                      columnchart
```

Section:
Explanation:
Box 1 =
SigninLogs
| where ResultType == 0
| summarize login_count = count() by identity
| render piechart
This query retrieves the sign-in logs, filters the successful sign-ins, summarizes the count of sign-ins per user, and renders the result as a pie chart.
Box 2 = Render

QUESTION 57
You have an Azure AD tenant that contains the users shown in the following table.



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

The User settings for enterprise applications have the following configuration.

- Users can consent to apps accessing company data on their behalf:
- Users can consent to apps accessing company data for the groups they
- Users can request admin consent to apps they are unable to consent to: Yes
- Who can review admin consent requests: Admin2, User2

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

A. User1

B. User2

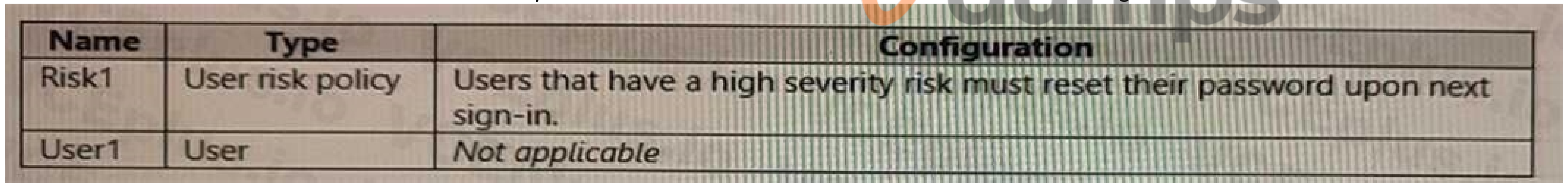
C. Admin1

D. Admin2

Correct Answer: C
Section:

QUESTION 58

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



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

Azure Multi-Factor Authentication (MFA) is enabled for all users.
User1 triggers a medium severity alert that requires additional investigation.
You need to force User1 to reset his password the next time he signs in. the solution must minimize administrative effort.
What should you do?

A. Configure a sign-in risk policy.

B. Mark User1 as compromised.

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

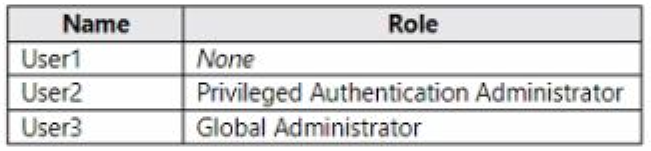
D. Reset the Azure MFA registration for User1.

Correct Answer: B
Section:

QUESTION 59

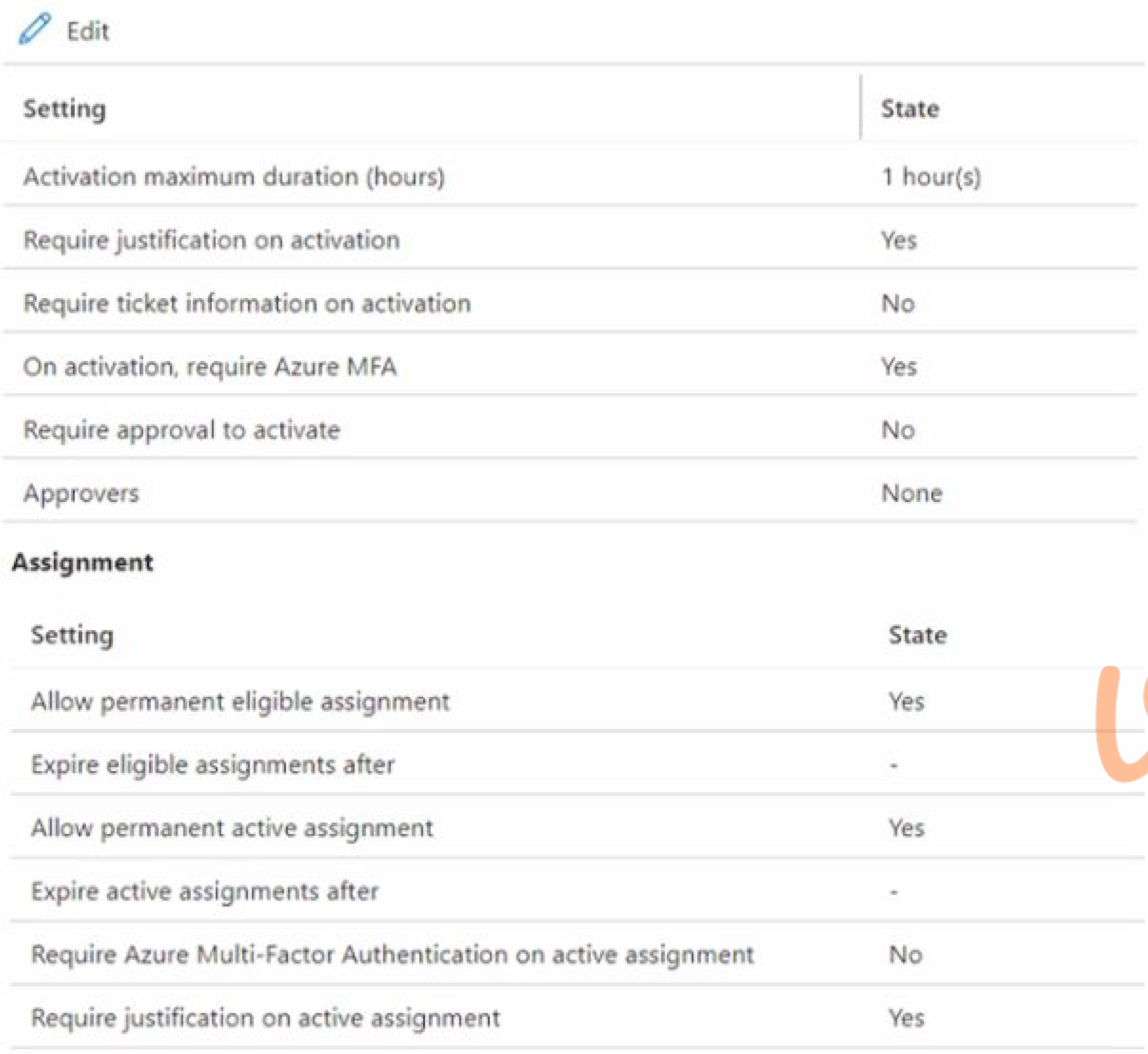
HOTSPOT

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.



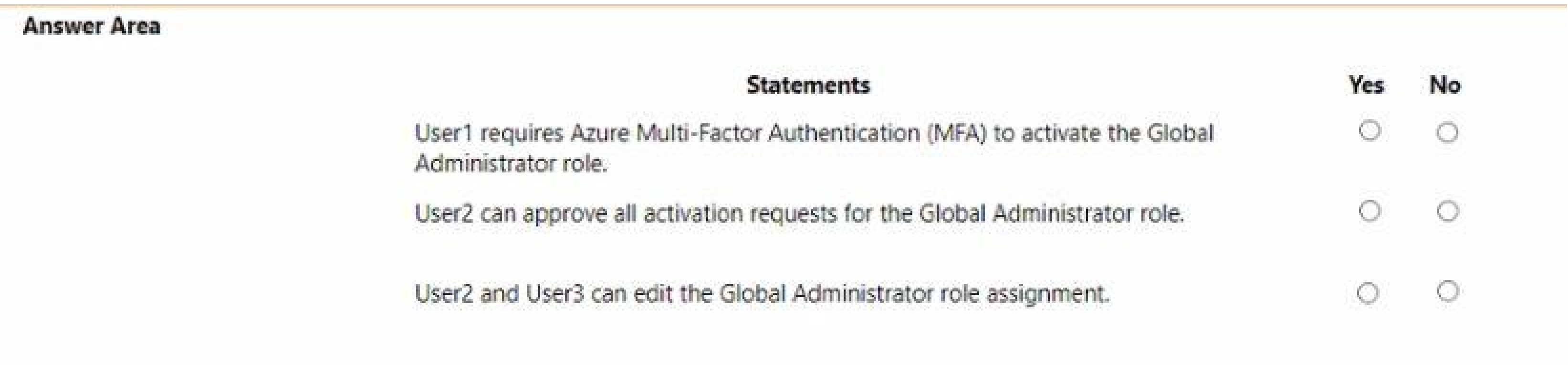
Setting	State
Activation maximum duration (hours)	1 hour(s)
Require justification on activation	Yes
Require ticket information on activation	No
On activation, require Azure MFA	Yes
Require approval to activate	No
Approvers	None

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.

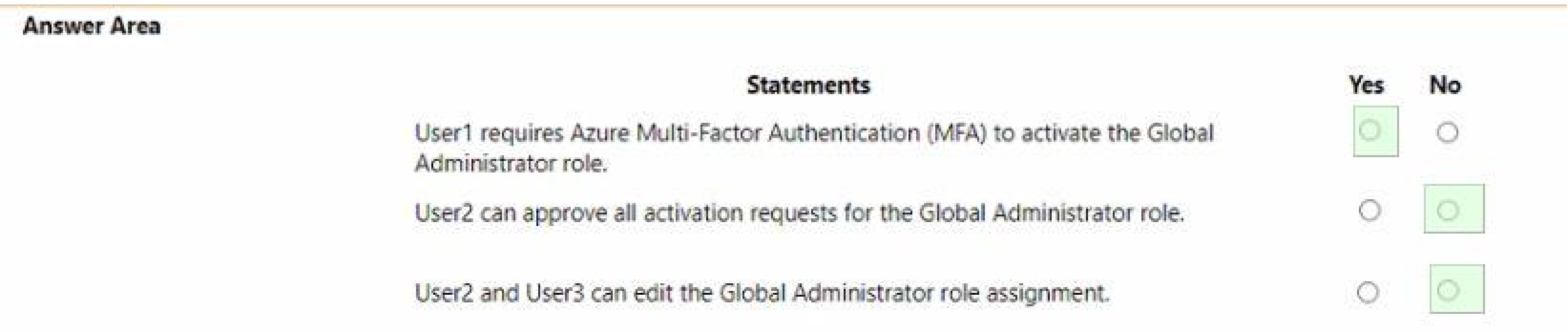
Hot Area:



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:

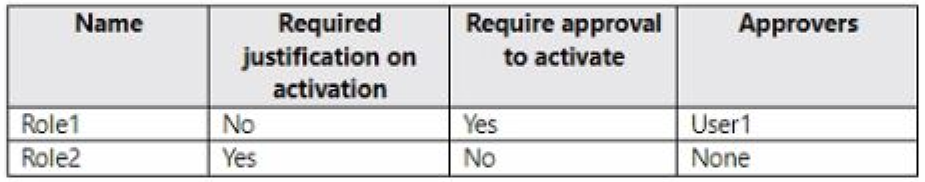


Answer Area

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.	○	[✓ ○]

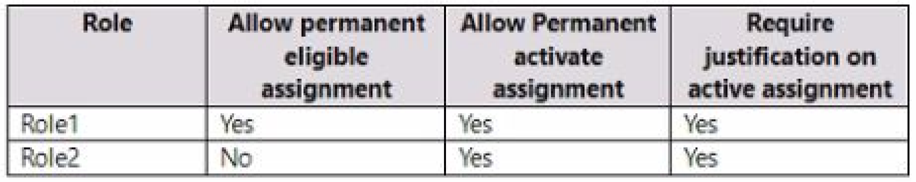
Section:
Explanation:

QUESTION 60
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.



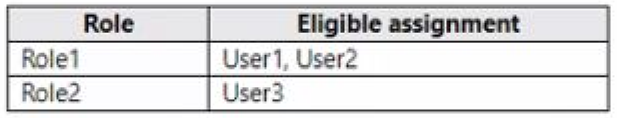
Name	Required justification on activation	Require approval to activate	Approvers
Role1	No	Yes	User1
Role2	Yes	No	None

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

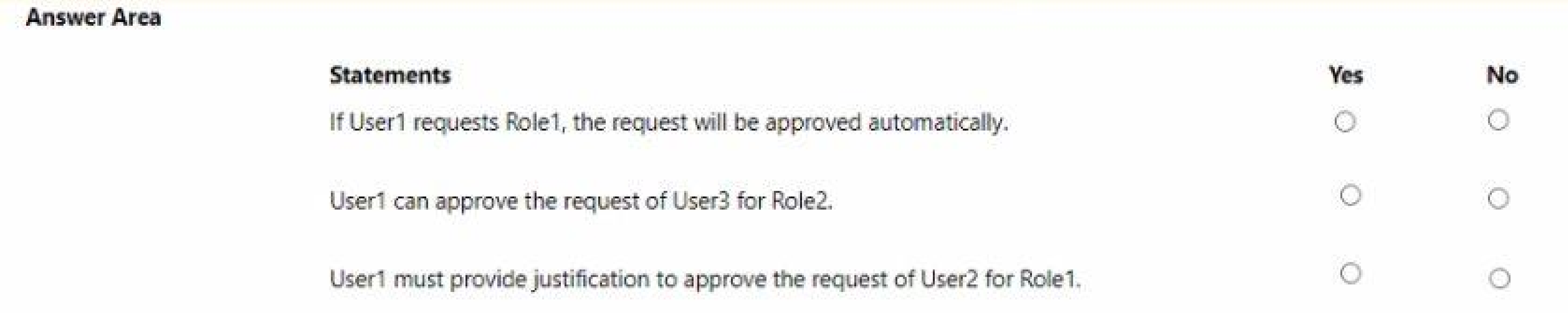
The Azure AD roles have the eligible users shown in the following table.



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.

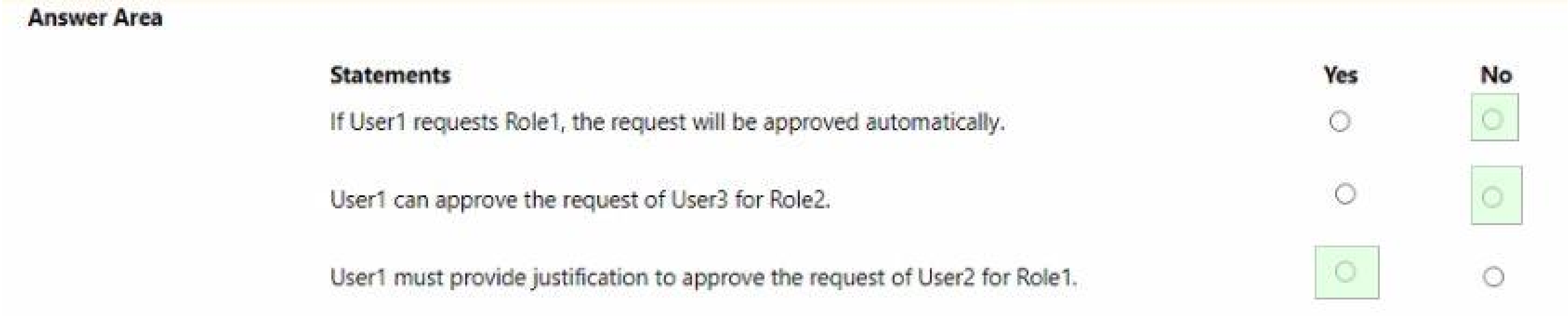
Hot Area:



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.	[✓ ○]	○

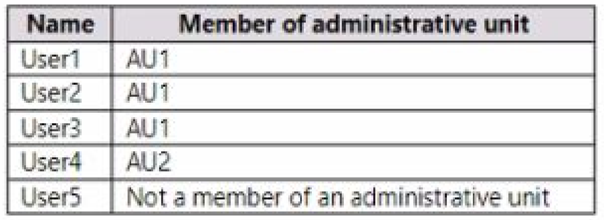
Section:
Explanation:

QUESTION 61
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

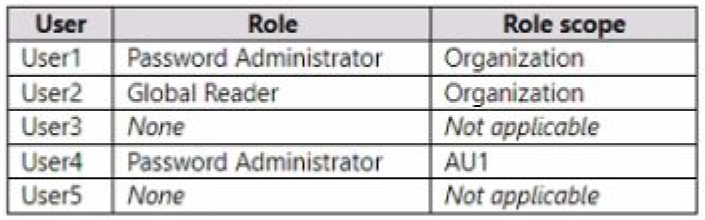
Correct Answer: B
Section:

QUESTION 62
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

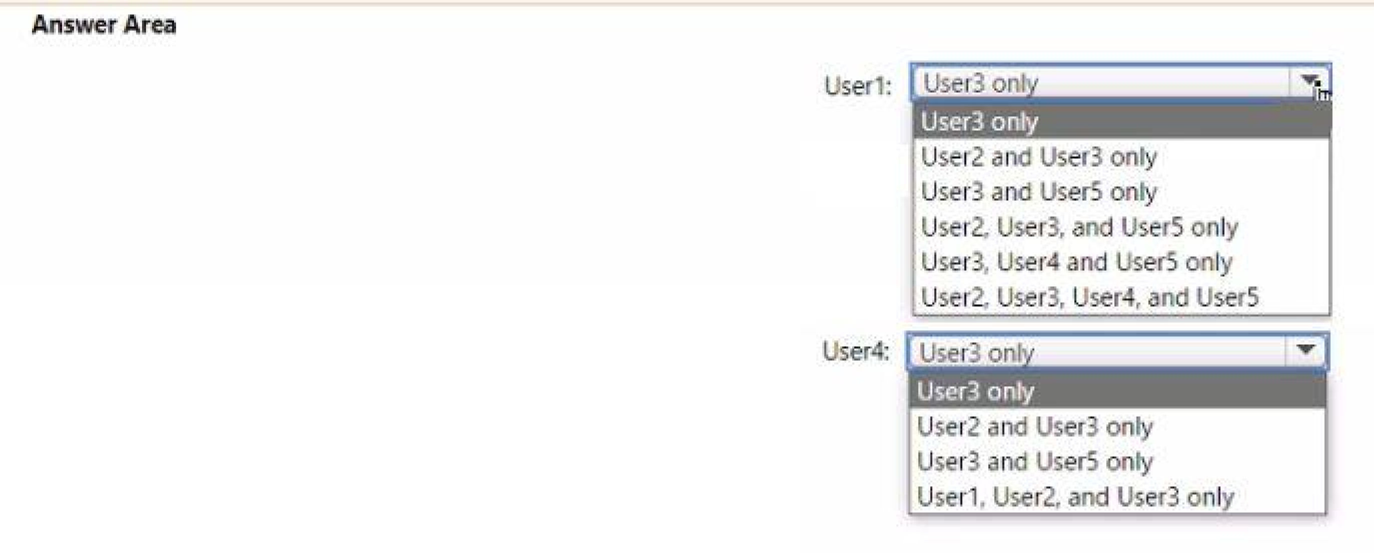
The users are assigned the roles shown in the following table.



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

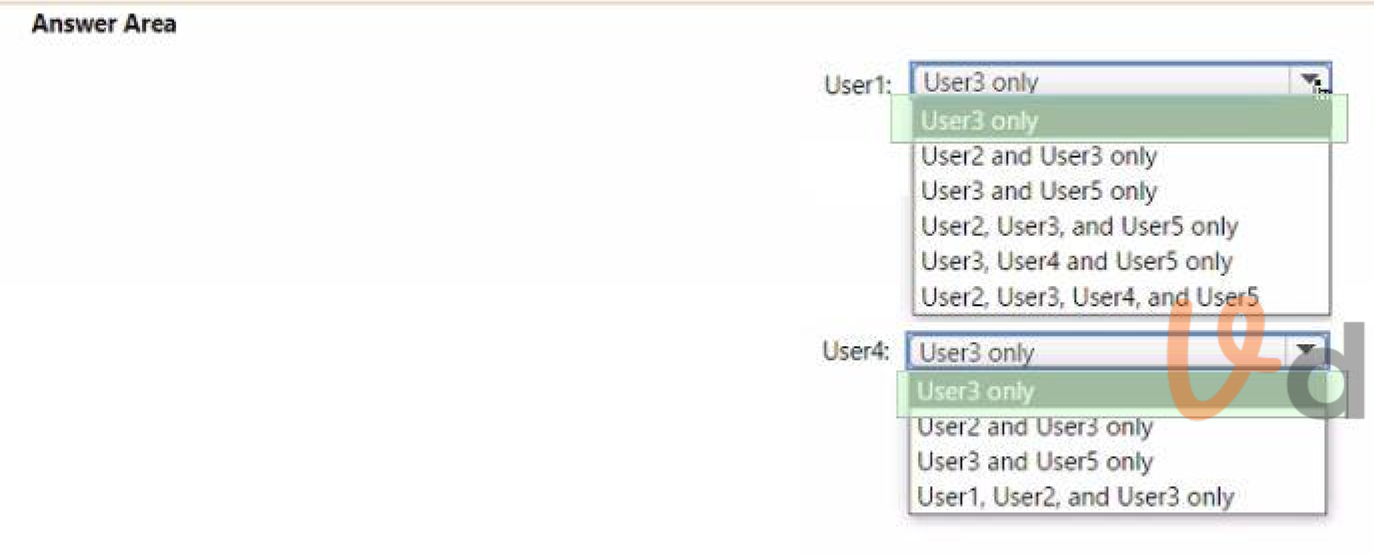
User1: User3 only

- 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

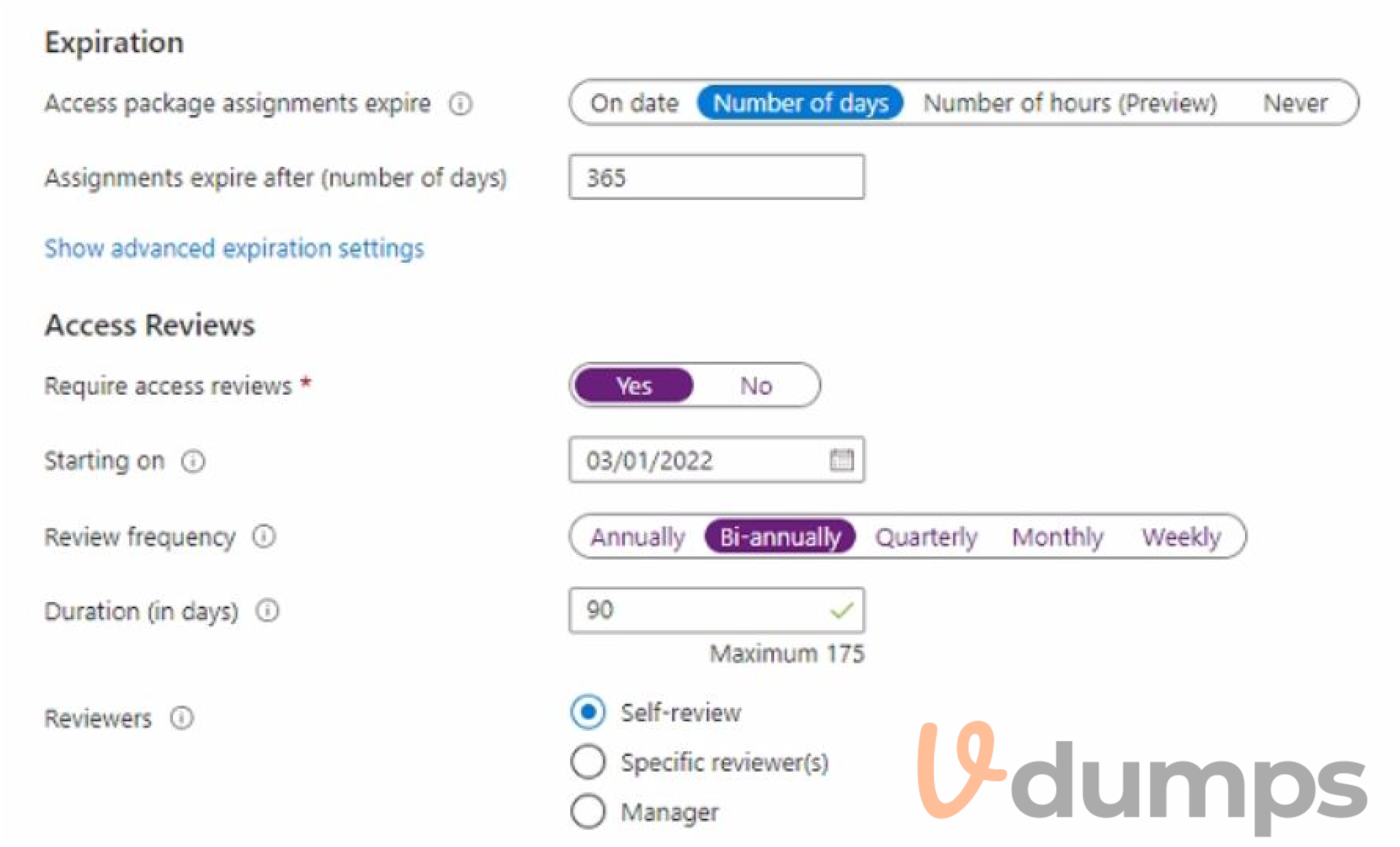
- User3 only
- User2 and User3 only
- User3 and User5 only
- User2, User3, and User5 only
- User3, User4 and User5 only
- User2, User3, User4, and User5

User4: User3 only

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

Section:
Explanation:

QUESTION 63
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:

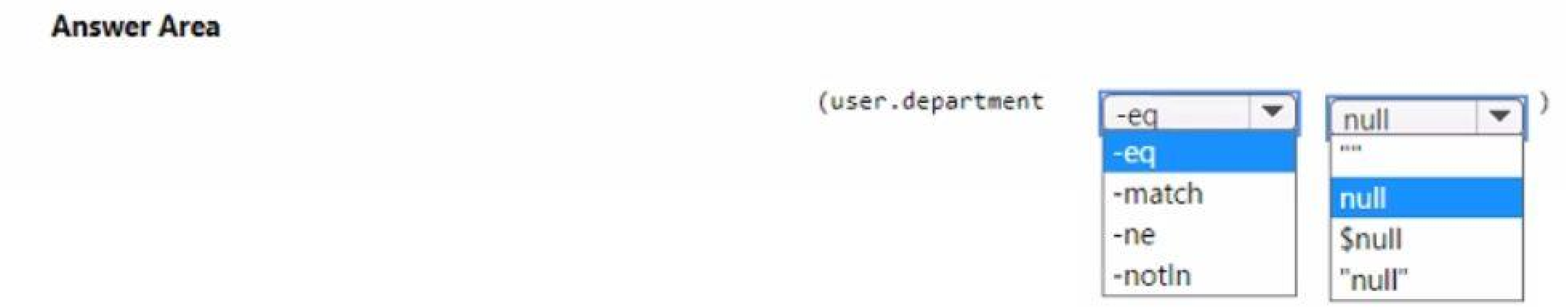
QUESTION 64
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps.
You need to identify which users access Facebook from their devices and browsers. The solution must minimize administrative effort.
What should you do first?

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 65
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.

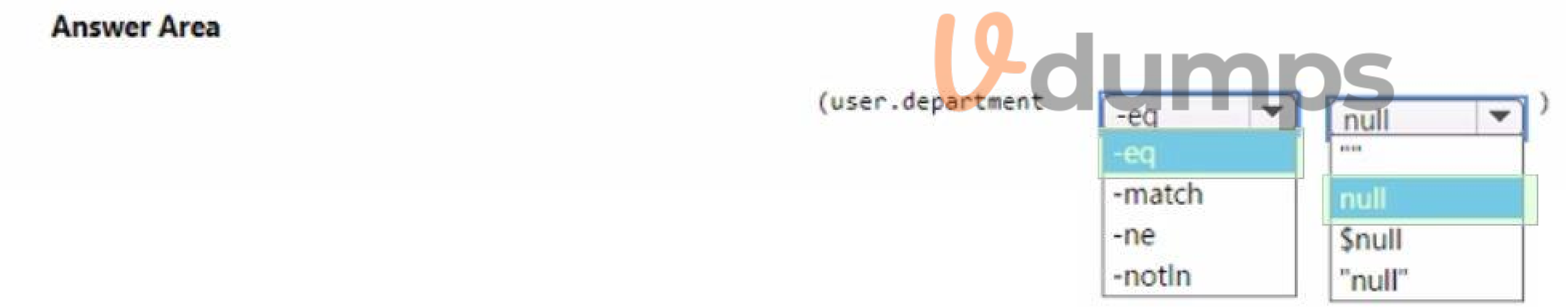
Hot Area:



Answer Area

(user.department [-eq ▼] [null ▼])

Answer Area:



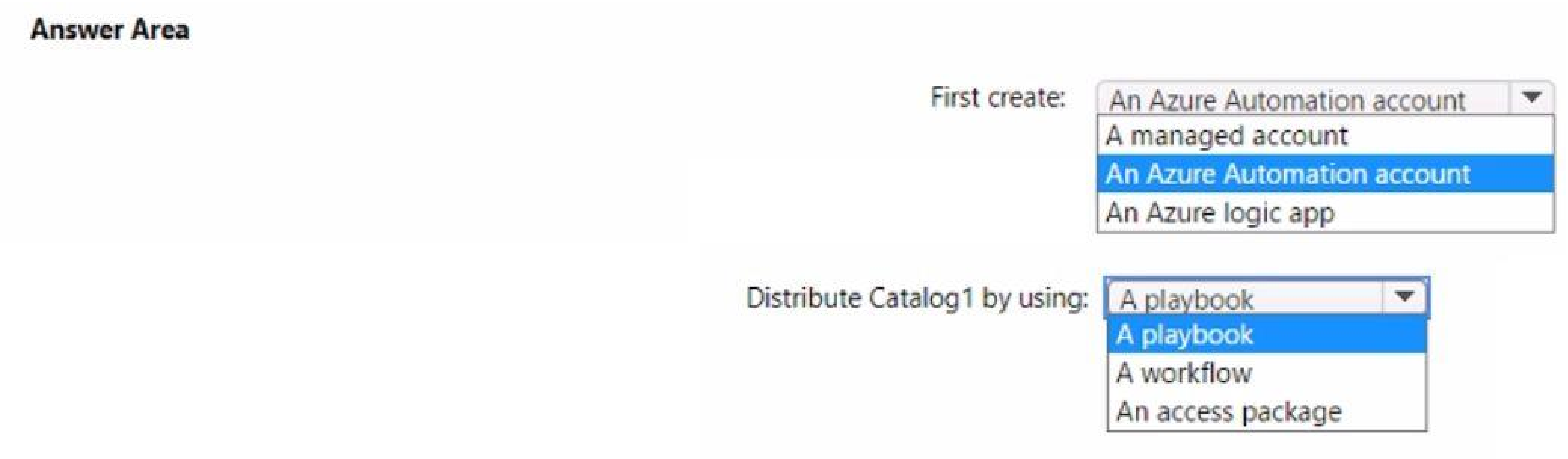
Answer Area

(user.department [-eq ▼] [null ▼])

Section:
Explanation:

QUESTION 66
HOTSPOT
You have an Azure subscription.
From Entitlement management, you plan to create a catalog named Catalog1 that will contain a custom extension.
What should you create first and what should you use to distribute Catalog1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

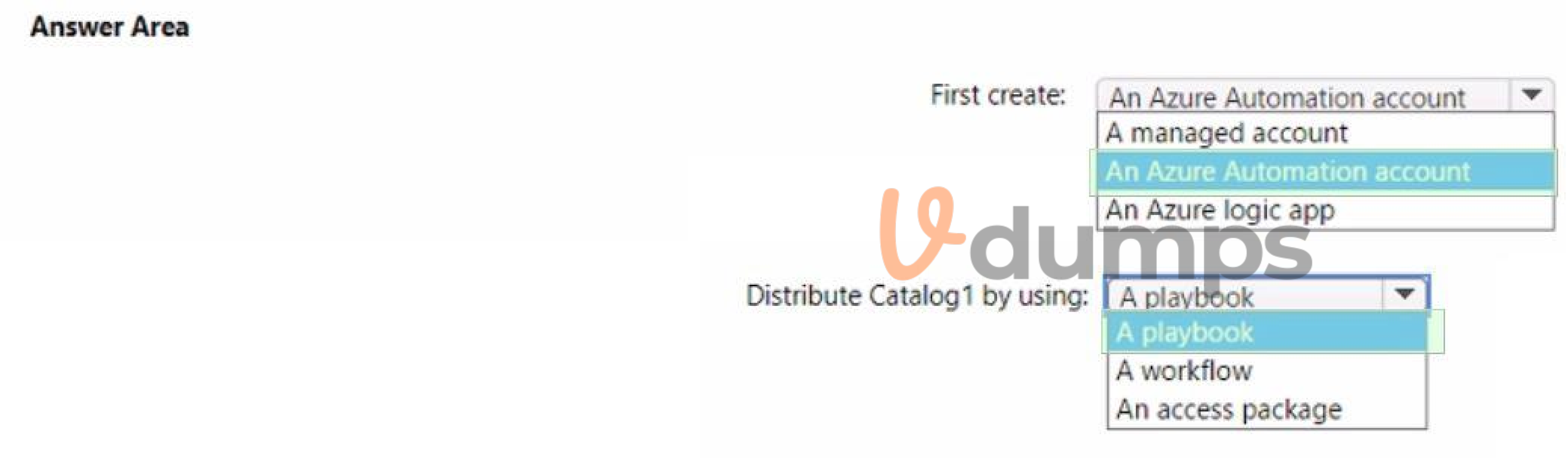
First create: An Azure Automation account

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

Distribute Catalog1 by using: A playbook

- A playbook
- A workflow
- An access package

Answer Area:



Answer Area

First create: An Azure Automation account

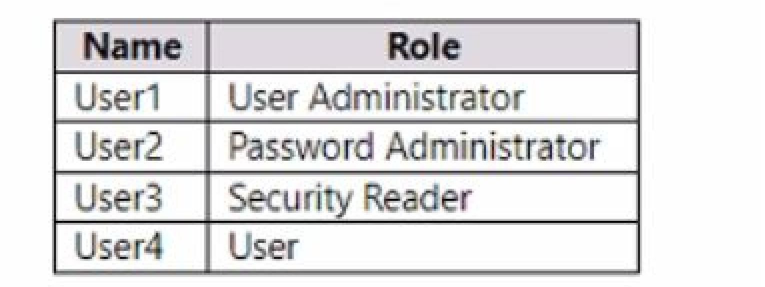
- A managed account
- An Azure Automation account
- An Azure logic app

Distribute Catalog1 by using: A playbook

- A playbook
- A workflow
- An access package

Section:
Explanation:

QUESTION 67
You have an Azure AD tenant that contains the users shown in The following table.



Name	Role
User1	User Administrator
User2	Password Administrator
User3	Security Reader
User4	User

You enable self-service password reset (SSPR) for all the users and configure SSPR to require security questions as the only authentication method.
Which users must use security questions when resetting their password?

A. User4 only

B. User3and User4only

C. User1 and User4only

D. User1, User3, and User4 only

E. User1, User2, User3. and User4

Correct Answer: B
Section:

QUESTION 68

You have an Azure AD tenant and a .NET web app named App1.
You need to register App1 for Azure AD authentication.
What should you configure for App1?

A. the executable name

B. the bundle ID

C. the package name

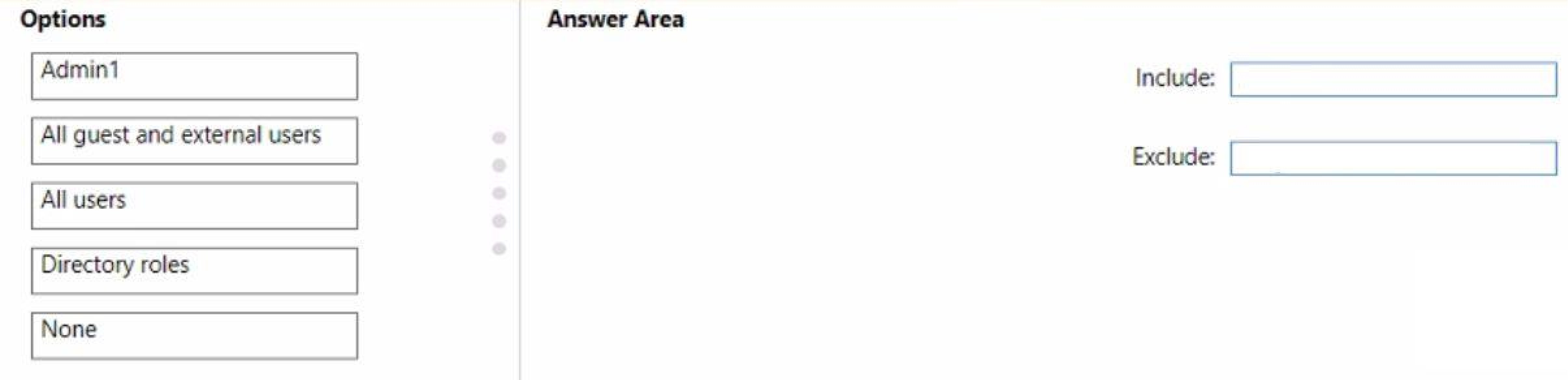
D. the redirect URI

Correct Answer: D
Section:

QUESTION 69

DRAG DROP
You have an Azure AD tenant that contains a user named Admin1.
Admin1 uses the Require password change for high-risk user's policy template to create a new Conditional Access policy.
Who is included and excluded by default in the policy assignment? To answer, drag the appropriate options to the correct target. Each option may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.

Select and Place:



Options

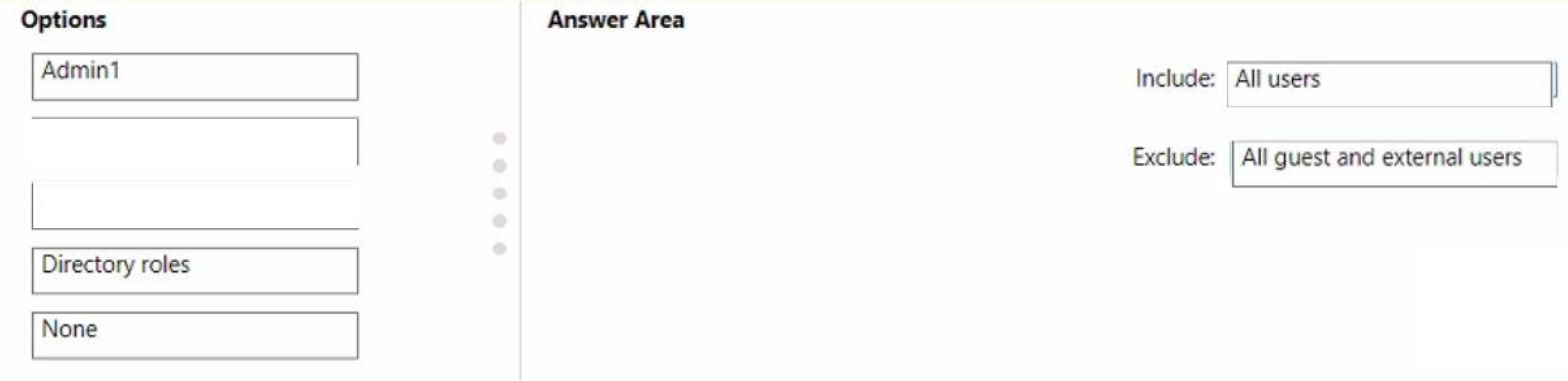
- Admin1
- All guest and external users
- All users
- Directory roles
- None

Answer Area

Include:

Exclude:

Correct Answer:



Options

Admin1

Directory roles

None

Answer Area

Include: All users

Exclude: All guest and external users

Section:
Explanation:

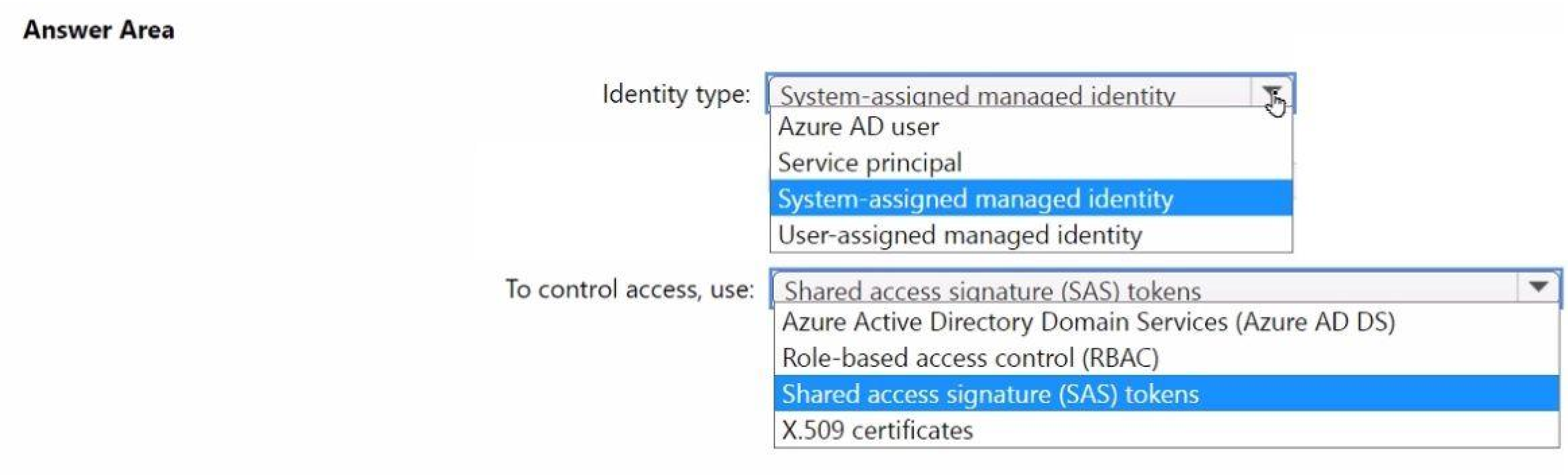
QUESTION 70
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After 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 an Amazon Web Services (AWS) account, a Google Workspace subscription, and a GitHub account.
You deploy an Azure subscription and enable Microsoft 365 Defender.
You need to ensure that you can monitor OAuth authentication requests by using Microsoft Defender for Cloud Apps.
Solution: From the Microsoft 365 Defender portal, you add the Amazon Web Services app connector.
Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section:

QUESTION 71
HOTSPOT
You have an Azure AD tenant that contains multiple storage accounts.
You plan to deploy multiple Azure App Service apps that will require access to the storage accounts.
You need to recommend an identity solution to provide the apps with access to the storage accounts. The solution must minimize administrative effort.
Which type of identity should you recommend, and what should you recommend using to control access to the storage accounts? To answer, select the appropriate options in the answer area.

Hot Area:

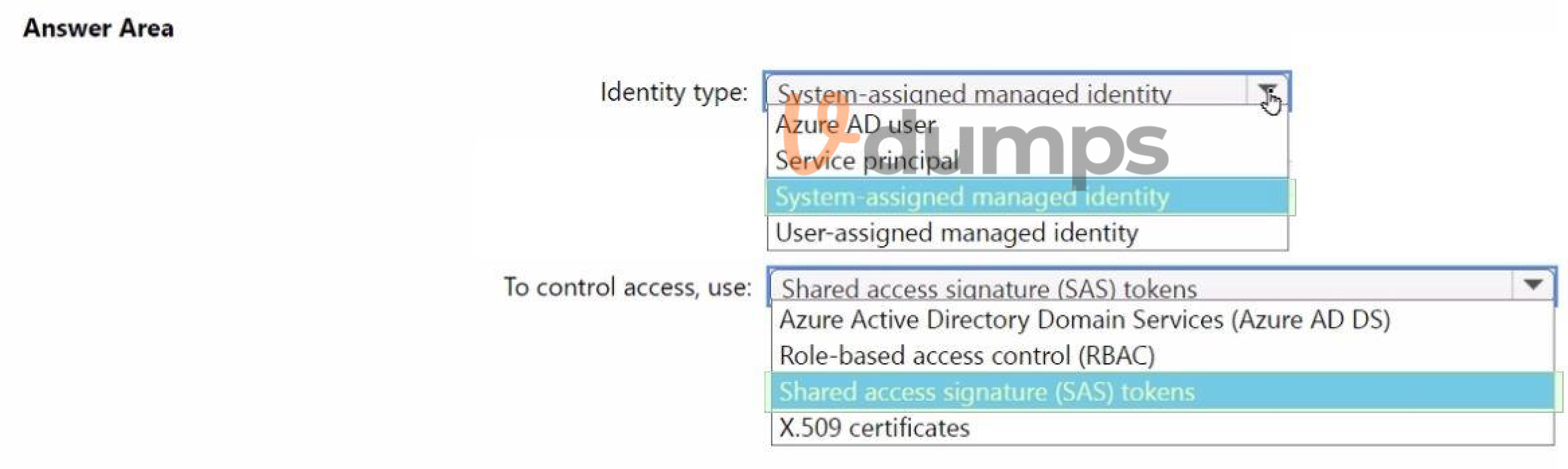


Answer Area

Identity type: System-assigned managed identity
- Azure AD user
- Service principal
- System-assigned managed identity
- User-assigned managed identity

To control access, use: Shared access signature (SAS) tokens
- Azure Active Directory Domain Services (Azure AD DS)
- Role-based access control (RBAC)
- Shared access signature (SAS) tokens
- X.509 certificates

Answer Area:



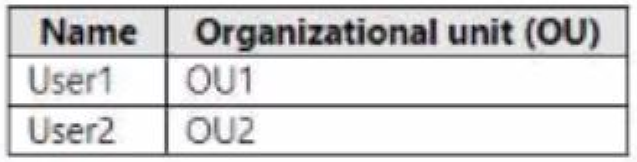
Answer Area

Identity type: System-assigned managed identity
- Azure AD user
- Service principal
- System-assigned managed identity
- User-assigned managed identity

To control access, use: Shared access signature (SAS) tokens
- Azure Active Directory Domain Services (Azure AD DS)
- Role-based access control (RBAC)
- Shared access signature (SAS) tokens
- X.509 certificates

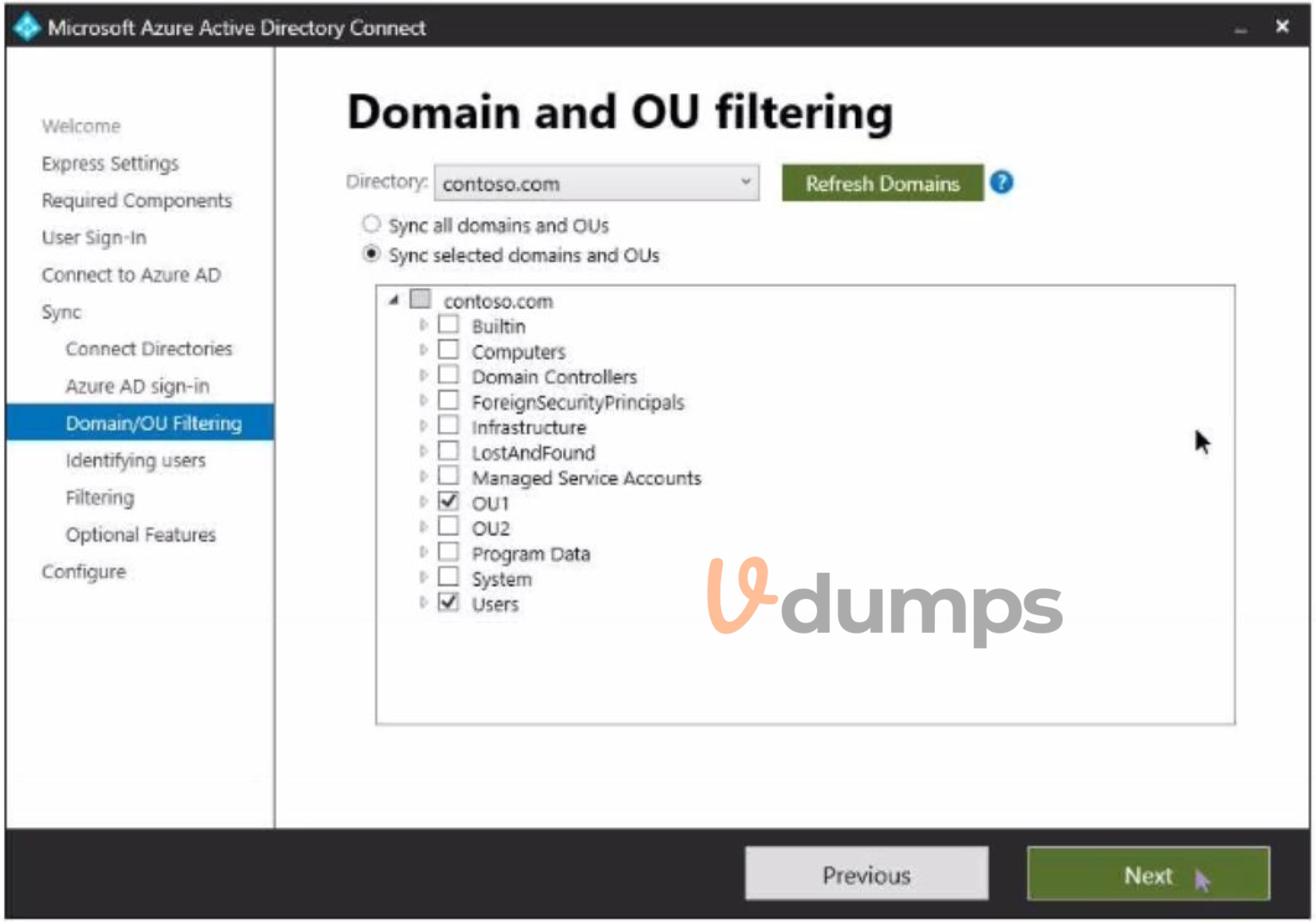
Section:
Explanation:

QUESTION 72
HOTSPOT
Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with Azure AD and contains the users shown in the following table.



Name	Organizational unit (OU)
User1	OU1
User2	OU2

In Azure AD Connect. Domain/OU Filtering is configured as shown in the following exhibit.



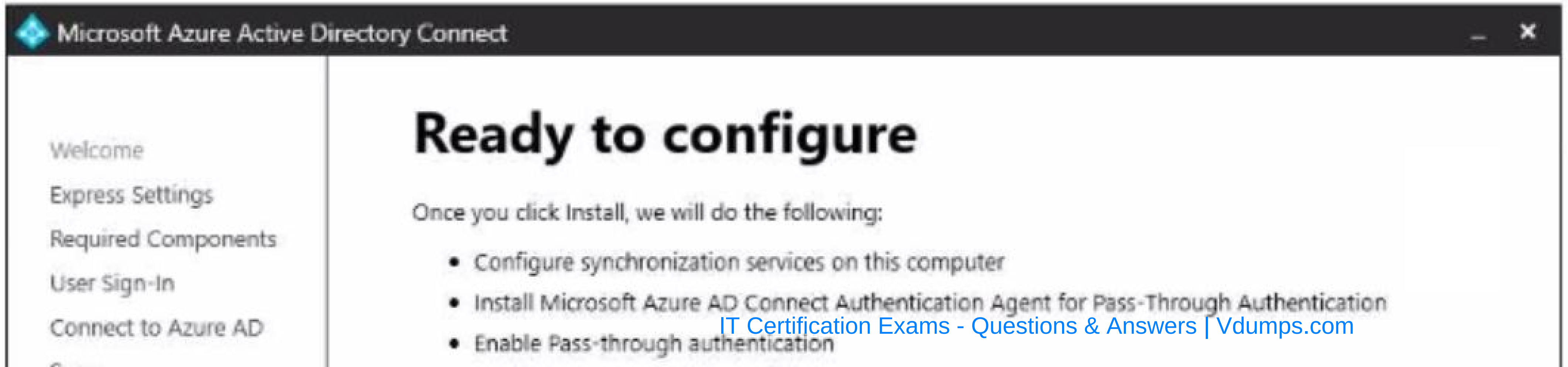
Domain and OU filtering

Directory: contoso.com

○ Sync all domains and OUs
● Sync selected domains and OUs

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

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



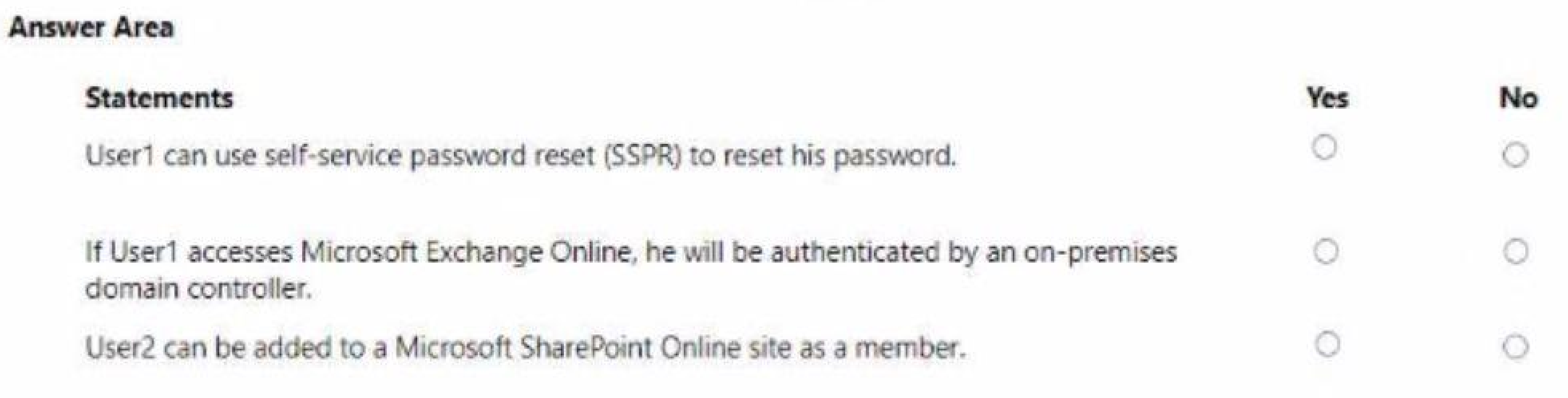
Ready to configure

Once you click Install, we will do the following:

- Configure synchronization services on this computer
- Install Microsoft Azure AD Connect Authentication Agent for Pass-Through Authentication
- Enable Pass-through authentication

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

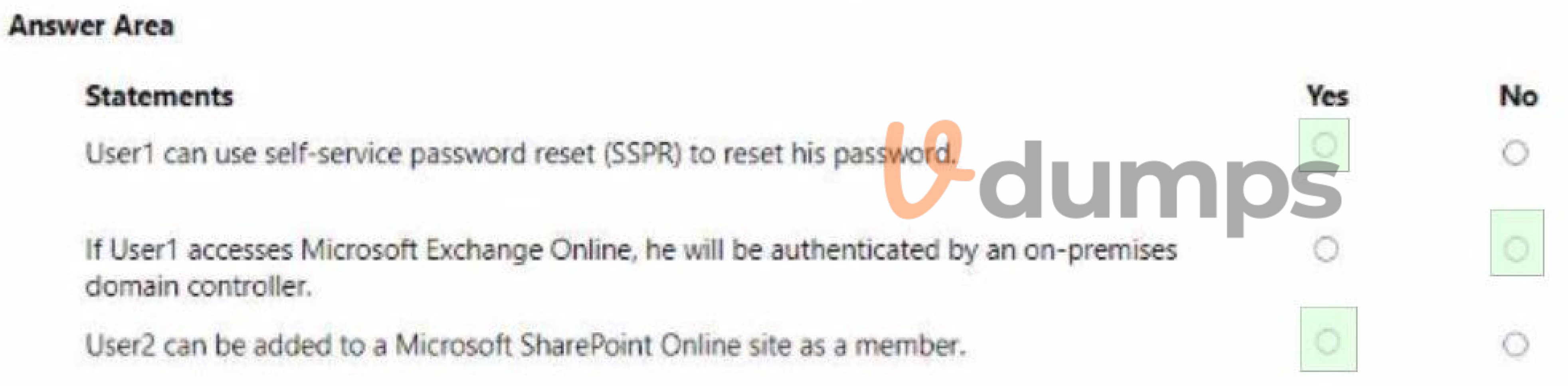
Hot Area:



Answer Area

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

Answer Area:



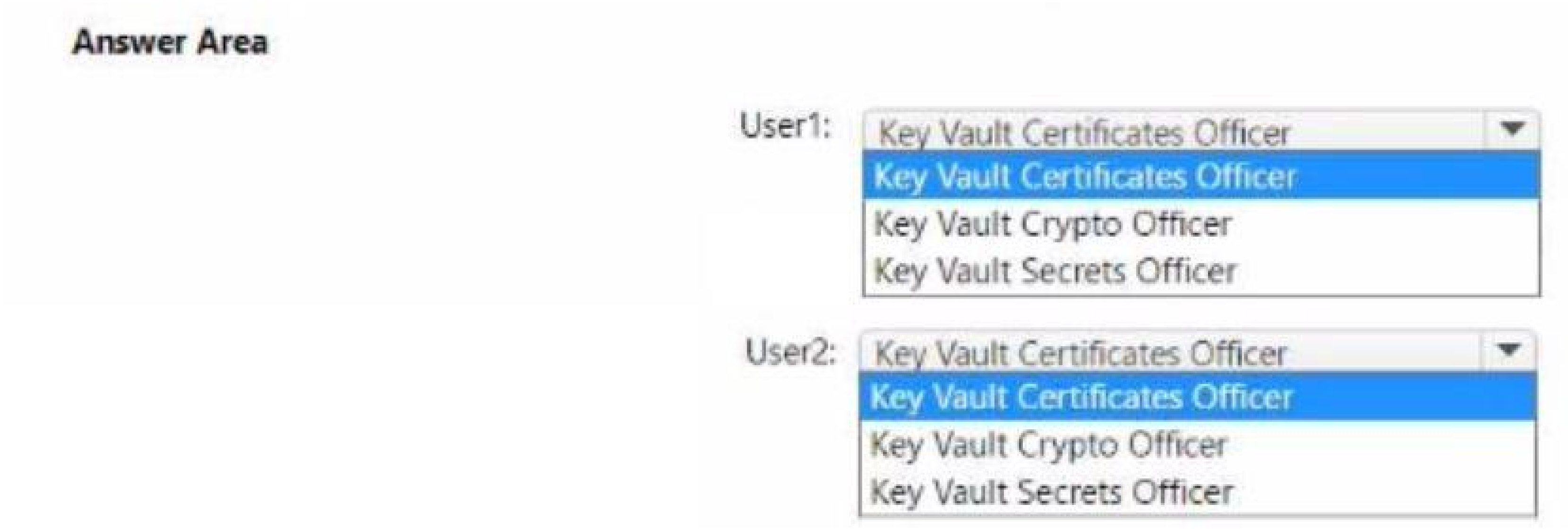
Answer Area

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

Section:
Explanation:

QUESTION 73
HOTSPOT
You have an Azure subscription that contains the resources shown in the following table.
You need to configure access to Vault1. The solution must meet the following requirements:
* Ensure that User1 can manage and create keys in Vault1.
* Ensure that User2 can access a certificate stored in Vault1.
* Use the principle of least privilege.
Which role should you assign to each user? To answer select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:

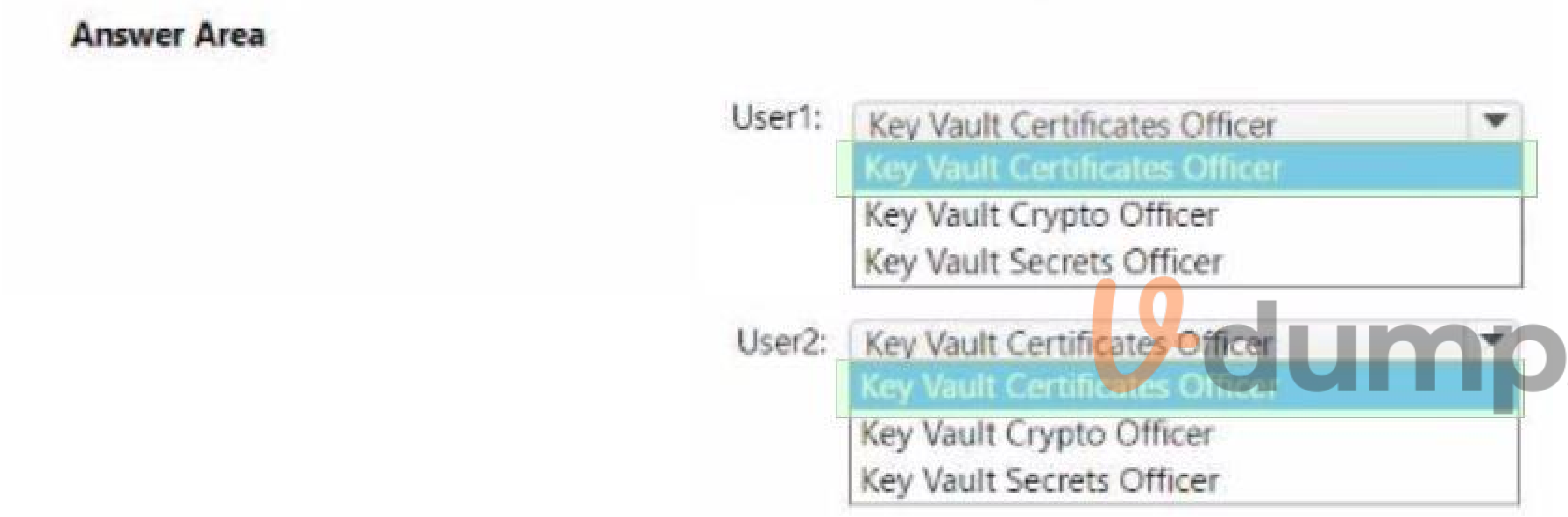


Answer Area

User1: Key Vault Certificates Officer
- Key Vault Certificates Officer
- Key Vault Crypto Officer
- Key Vault Secrets Officer

User2: Key Vault Certificates Officer
- Key Vault Certificates Officer
- Key Vault Crypto Officer
- Key Vault Secrets Officer

Answer Area:



Answer Area

User1: Key Vault Certificates Officer
- Key Vault Certificates Officer
- Key Vault Crypto Officer
- Key Vault Secrets Officer

User2: Key Vault Certificates Officer
- Key Vault Certificates Officer
- Key Vault Crypto Officer
- Key Vault Secrets Officer

Section:
Explanation:

QUESTION 74
You have a Microsoft 365 E5 subscription.
You purchase the app governance add-on license.
You need to enable app governance integration.
Which portal should you use?

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

Correct Answer: A
Section:

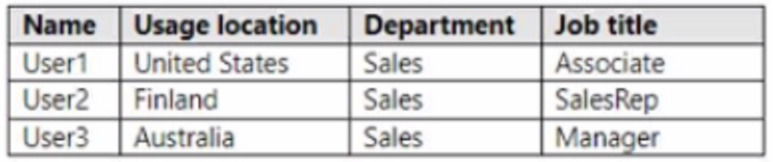
QUESTION 75

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.

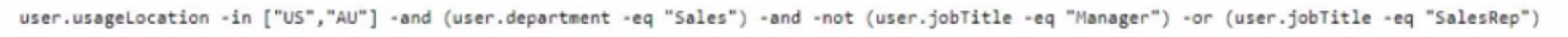
Correct Answer: A
Section:

QUESTION 76
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 77
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:

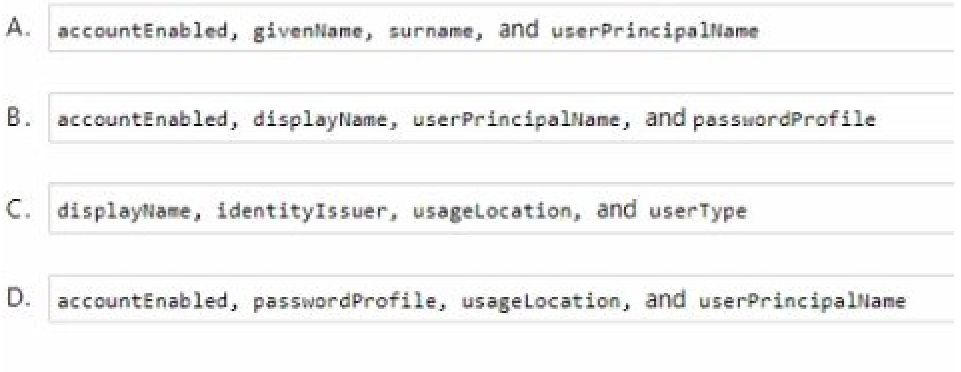
QUESTION 78

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 79
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 80
You have an Azure AD tenant that contains a user named User1
User1 needs to manage license assignments and reset user passwords.
Which role should you assign to User1?

A. License administrator
B. Helpdesk administrator
C. Billing administrator
D. User administrator

Correct Answer: D
Section:

QUESTION 81

You have an Azure AD tenant that has multi-factor authentication (MFA) enforced and self-service password reset (SSPR) enabled.
You enable combined registration in interrupt mode.
You create a new user named User1.
Which two authentication methods can User1 use to complete the combined registration process? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. a FID02 security key
B. a hardware token
C. a one-time passcode email
D. Windows Hello for Business
E. the Microsoft Authenticator app

Correct Answer: A, E
Section:

QUESTION 82
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 83
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 84

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?

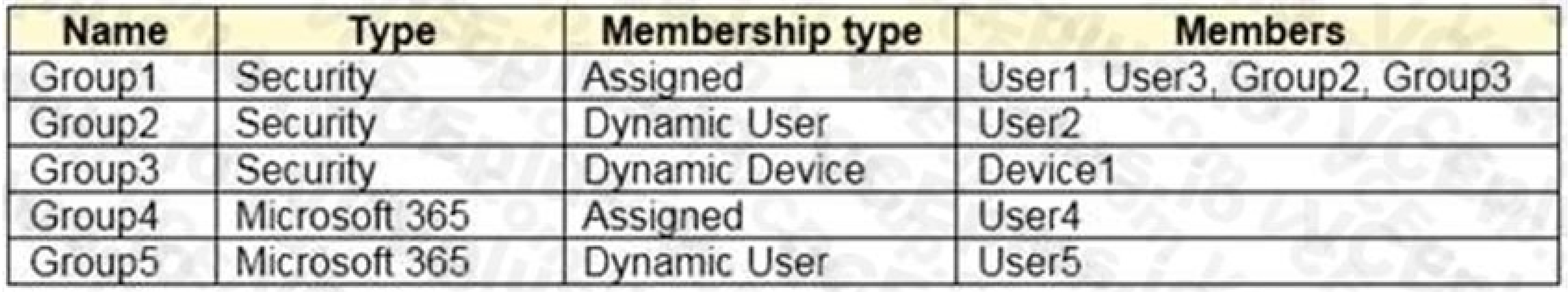
A. Yes

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 85

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

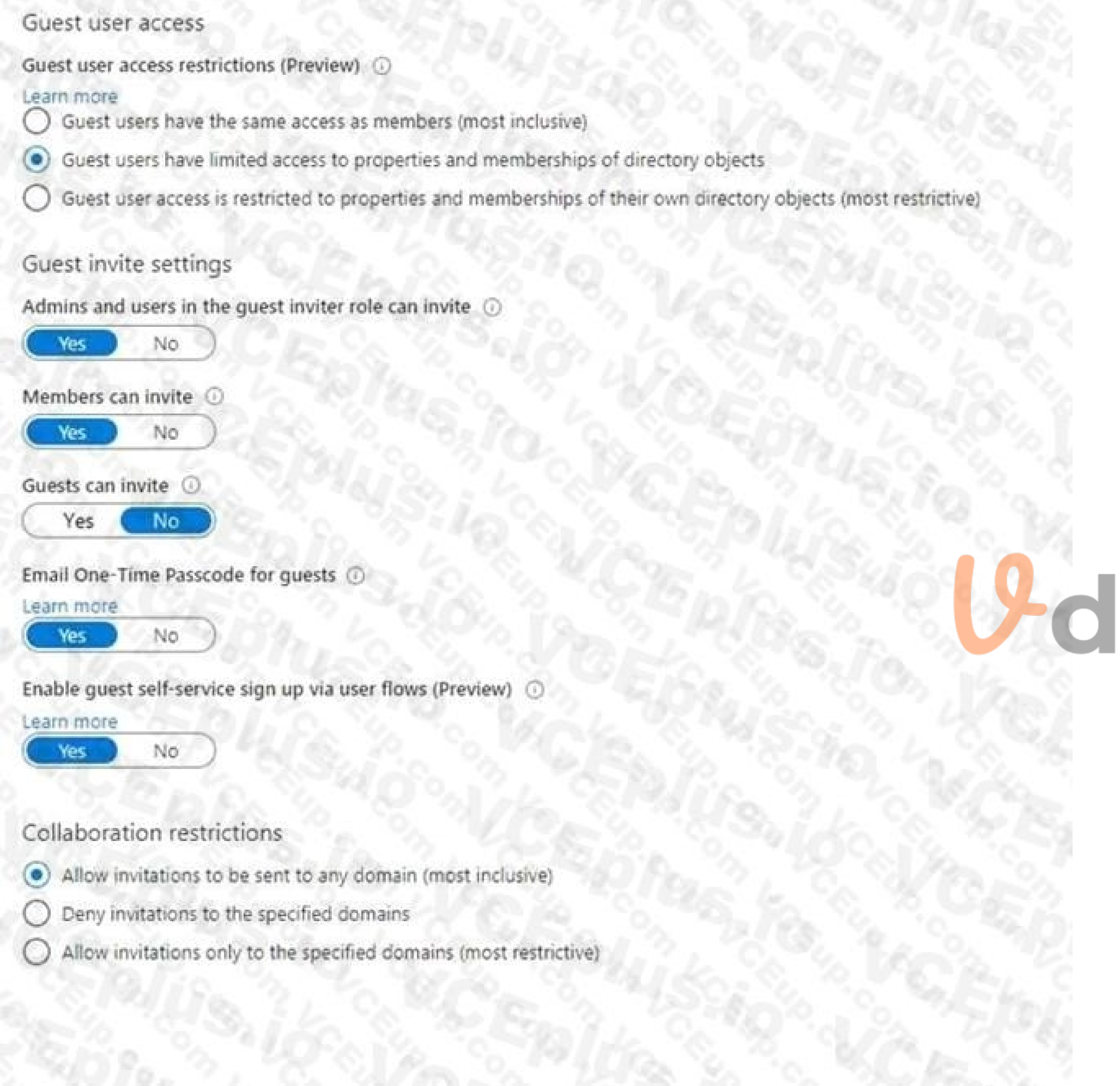
D. Group1 only

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 86
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

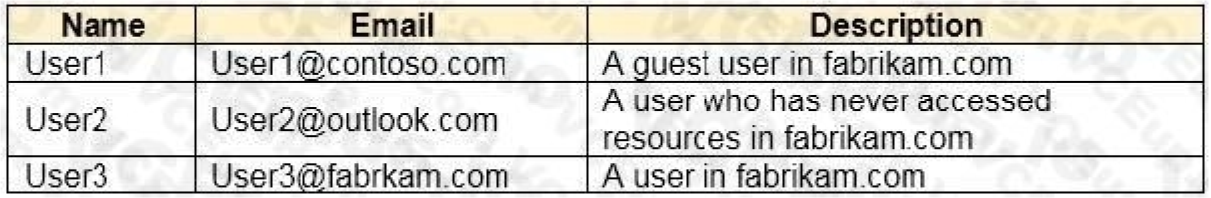
Guests can invite ⓘ
Yes [✓ No]

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 87
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 88
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

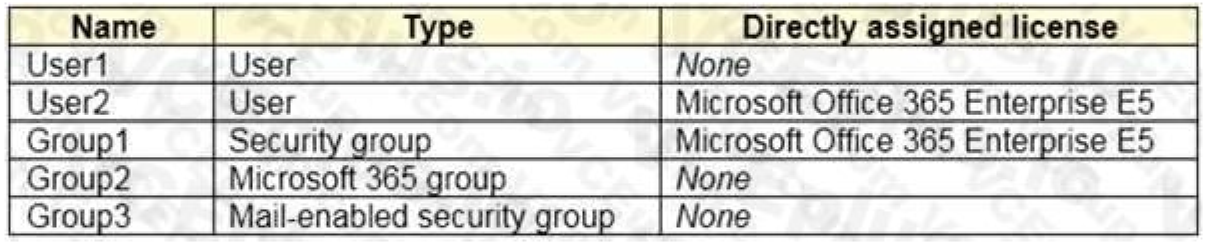
C. username

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 89
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 90
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 91
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 92

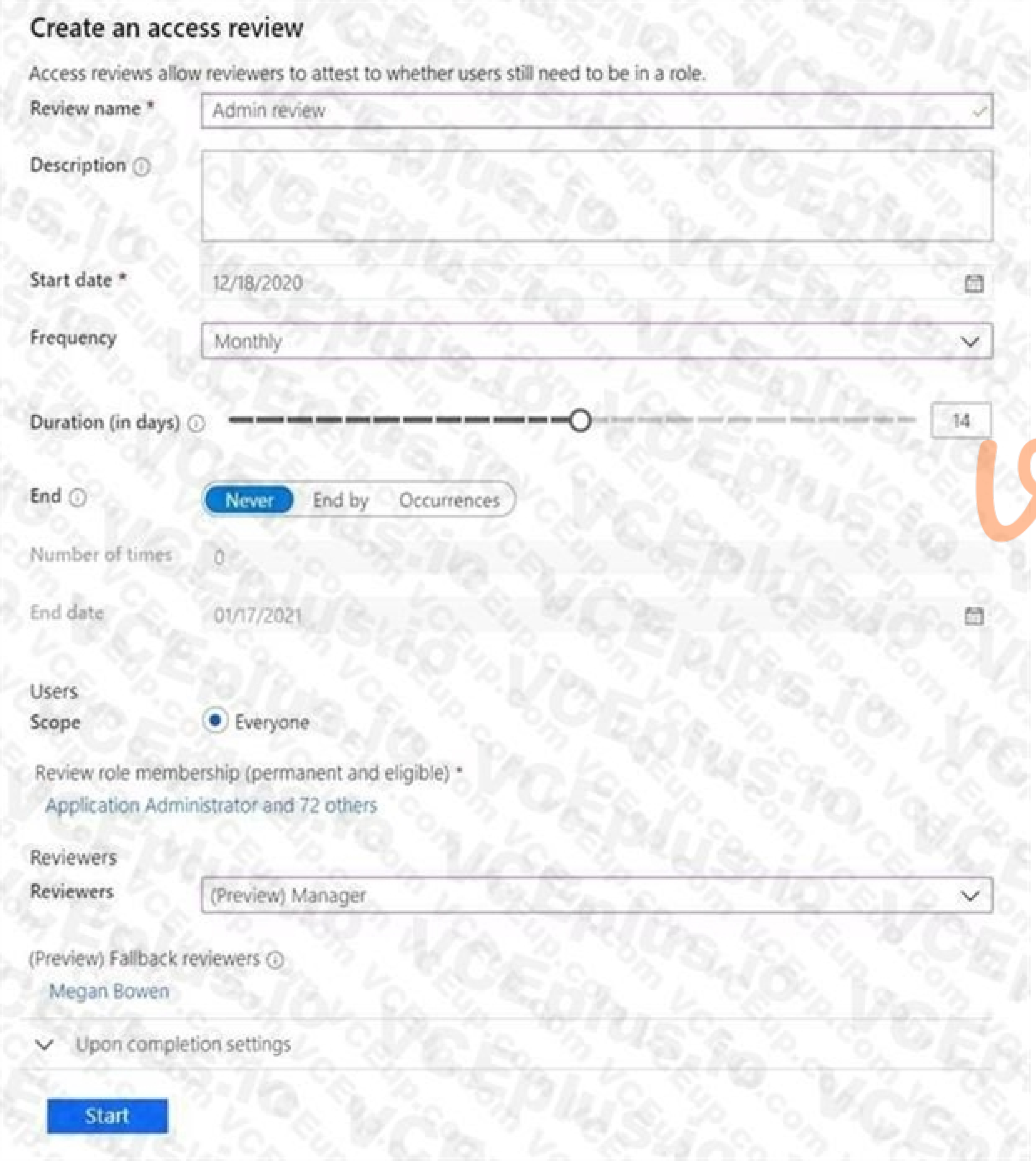
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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.

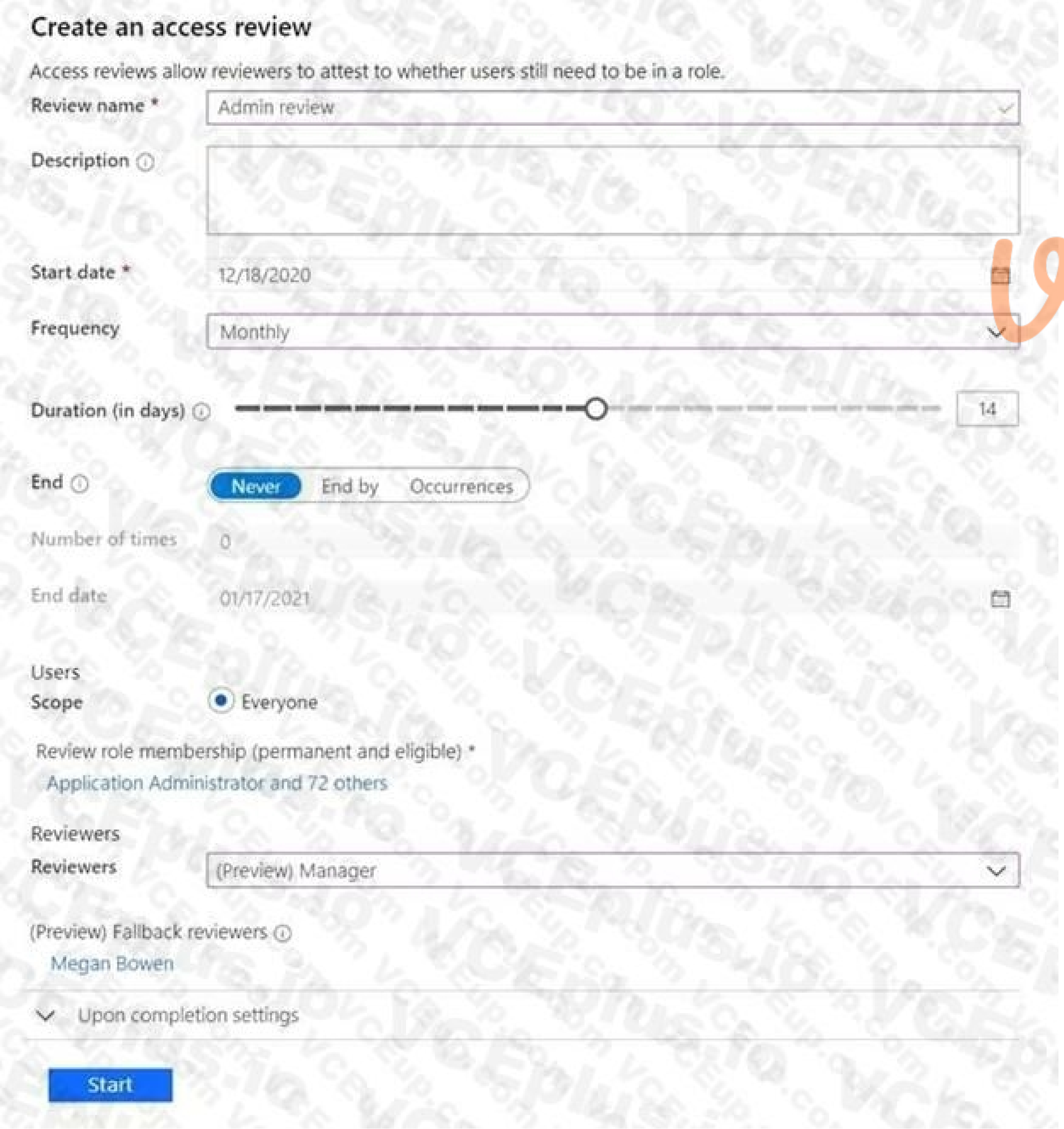
Solution: You create a separate access review for each role.

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 93
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

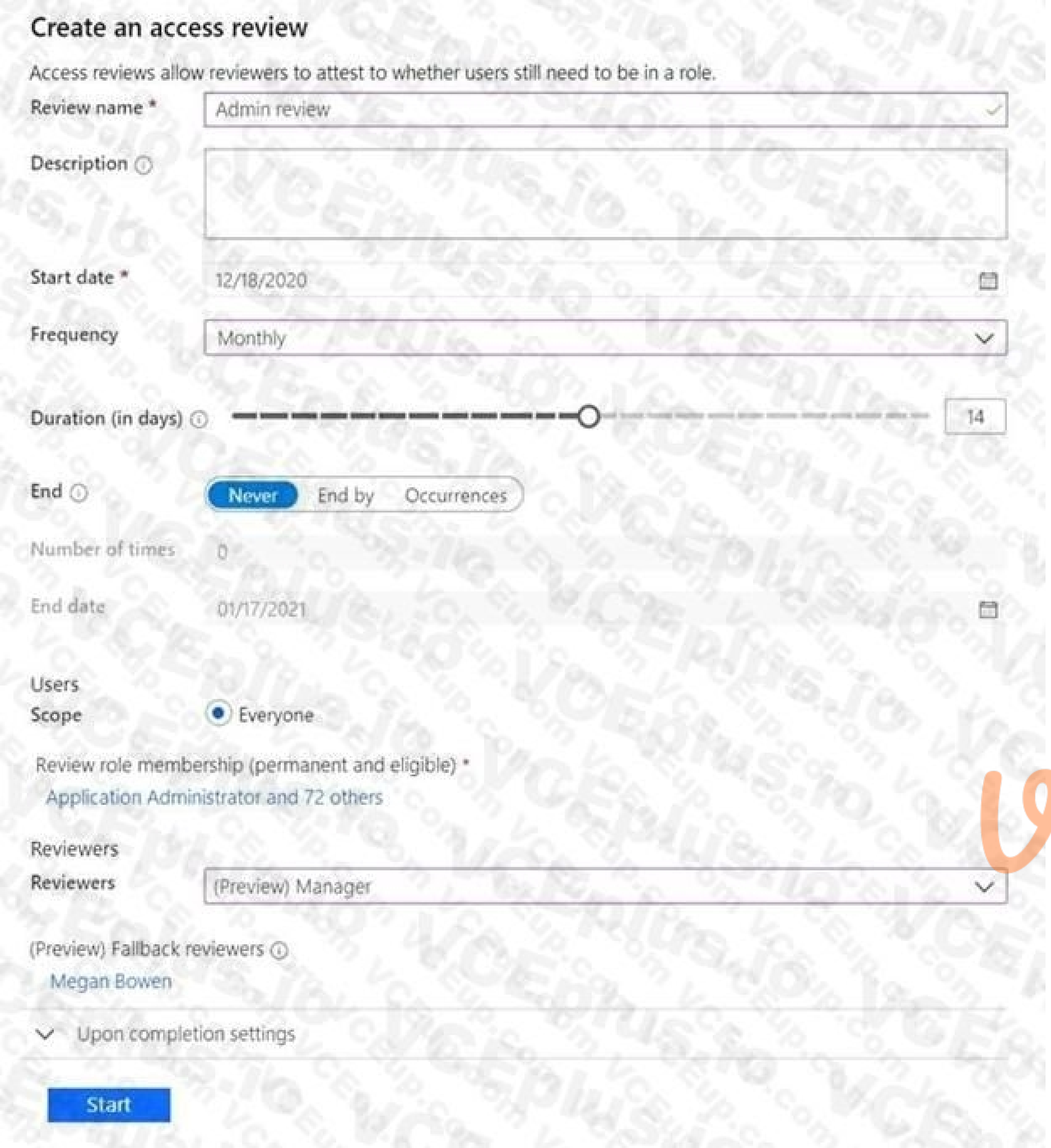
You discover that all access review requests are received by Megan Bowen.
You need to ensure that the manager of each department receives the access reviews of their respective department.
Solution: You modify the properties of the IT administrator user accounts.
Does this meet the goal?

A. Yes

B. No

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

QUESTION 94
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 set Reviewers to Member (self).
Does this meet the goal?

A. Yes

B. No

Correct Answer: B
Section:

QUESTION 95

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 96
Your network contains an Active Directory forest named contoso.com that is linked to an Azure Active Directory (Azure AD) tenant named contoso.com by using Azure AD Connect.
You need to prevent the synchronization of users who have the extensionAttribute15 attribute set to NoSync.
What should you do in Azure AD Connect?

A. Create an inbound synchronization rule for the Windows Azure Active Directory connector.
B. Configure a Full Import run profile.
C. Create an inbound synchronization rule for the Active Directory Domain Services connector.
D. Configure an Export run profile.

Correct Answer: C
Section:
Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-change-theconfiguration

QUESTION 97
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps and Conditional Access policies. You need to block access to cloud apps when a user is assessed as high risk.
Which type of policy should you create in the Microsoft Defender for Cloud Apps?

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

Correct Answer: C
Section:

QUESTION 98
SIMULATION 6
You need to implement additional security checks before the members of the Sg-Executive can access any company apps. The members must meet one of the following conditions:
* Connect by using a device that is marked as compliant by Microsoft Intune.
* Connect by using client apps that are protected by app protection policies.

A. See the Explanation for the complete step by step solution

Correct Answer: A
Section:
Explanation:
To implement additional security checks for the Sg-Executive group members before they can access any company apps, you can use Conditional Access policies in Microsoft Entra. Here's a step-by-step guide:
Sign in to the Microsoft Entra admin center:
Ensure you have the role of Global Administrator or Security Administrator.
Navigate to Conditional Access:
Go to Security > Conditional Access.
Create a new policy:
Select + New policy.
Name the policy appropriately, such as ''Sg-Executive Security Checks''.
Assign the policy to the Sg-Executive group:
Under Assignments, select Users and groups.
Choose Select users and groups and then Groups.
Search for and select the Sg-Executive group.
Define the application control conditions:
Under Cloud apps or actions, select All cloud apps to apply the policy to any company app.
Set the device compliance requirement:
Under Conditions > Device state, configure the policy to include devices marked as compliant by Microsoft Intune.
Set the app protection policy requirement:
Under Conditions > Client apps, configure the policy to include client apps that are protected by app protection policies.
Configure the access controls:
Under Access controls > Grant, select Grant access.
Choose Require device to be marked as compliant and Require approved client app.
Ensure that the option Require one of the selected controls is enabled.
Enable the policy:
Set Enable policy to On.
Review and save the policy:
Review all settings to ensure they meet the requirements.
Click Create to save and implement the policy.
By following these steps, you will ensure that the Sg-Executive group members can only access company apps if they meet one of the specified conditions, either by using a compliant device or a protected client app. This enhances the security posture of your organization by enforcing stricter access controls for executive-level users.

QUESTION 99
SIMULATION 7
You need to lock out accounts for five minutes when they have 10 failed sign-in attempts.

A. See the Explanation for the complete step by step solution

Correct Answer: A
Section:
Explanation:
To configure the account lockout settings so that accounts are locked out for five minutes after 10 failed sign-in attempts, you can follow these steps:
Open the Microsoft Entra admin center:
Sign in with an account that has the Security Administrator or Global Administrator role.
Navigate to the lockout settings:
Go to Security > Authentication methods > Password protection.
Adjust the Smart Lockout settings:
Set the Lockout threshold to 10 failed sign-in attempts.
Set the Lockout duration (in minutes) to 5.

Please note that by default, smart lockout locks an account from sign-in after 10 failed attempts in Azure Public and Microsoft Azure operated by 21Vianet tenants1. The lockout period is one minute at first, and longer in subsequent attempts. However, you can customize these settings to meet your organization's requirements if you have Microsoft Entra ID P1 or higher licenses for your users

QUESTION 100
SIMULATION 8
You need to prevent all users from using legacy authentication protocols when authenticating to Microsoft Entra ID.

A. See the Explanation for the complete step by step solution

Correct Answer: A
Section:
Explanation:
To prevent all users from using legacy authentication protocols when authenticating to Microsoft Entra ID, you can create a Conditional Access policy that blocks legacy authentication. Here's how to do it:
Sign in to the Microsoft Entra admin center:
Ensure you have the role of Global Administrator or Conditional Access Administrator.
Navigate to Conditional Access:
Go to Security > Conditional Access.
Create a new policy:
Select + New policy.
Give your policy a name that reflects its purpose, like ''Block Legacy Auth''.
Set users and groups:
Under Assignments, select Users or workload identities.
Under Include, select All users.
Under Exclude, select Users and groups and choose any accounts that must maintain the ability to use legacy authentication. It's recommended to exclude at least one account to prevent lockout1.
Target resources:
Under Cloud apps or actions, select All cloud apps.
Set conditions:
Under Conditions > Client apps, set Configure to Yes.
Check only the boxes for Exchange ActiveSync clients and Other clients.
Configure access controls:
Under Access controls > Grant, select Block access.
Enable policy:
Confirm your settings and set Enable policy to Report-only initially to understand the impact.
After confirming the settings using report-only mode, you can move the Enable policy toggle from Report-only to On2.
By following these steps, you will block legacy authentication protocols for all users, enhancing the security posture of your organization by requiring modern authentication methods. Remember to monitor the impact of this policy and adjust as necessary to ensure business continuity.