

Microsoft.SC-300.vDec-2023.by.Jacky.85q

Number: SC-300  
Passing Score: 800  
Time Limit: 120  
File Version: 4.0

Website: [www.VCEplus.io](http://www.VCEplus.io)

Exam Code: SC-300

Twitter: [https://twitter.com/VCE\\_Plus](https://twitter.com/VCE_Plus)

Exam Name: Microsoft Identity and Access Administrator



## Case Study 02

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 Fabricam 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\_Resourecs 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 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 2

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 3

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:**

[www.VCEplus.io](https://www.VCEplus.io)

### 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 4

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 5

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 6**

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

**QUESTION 7**

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 8**

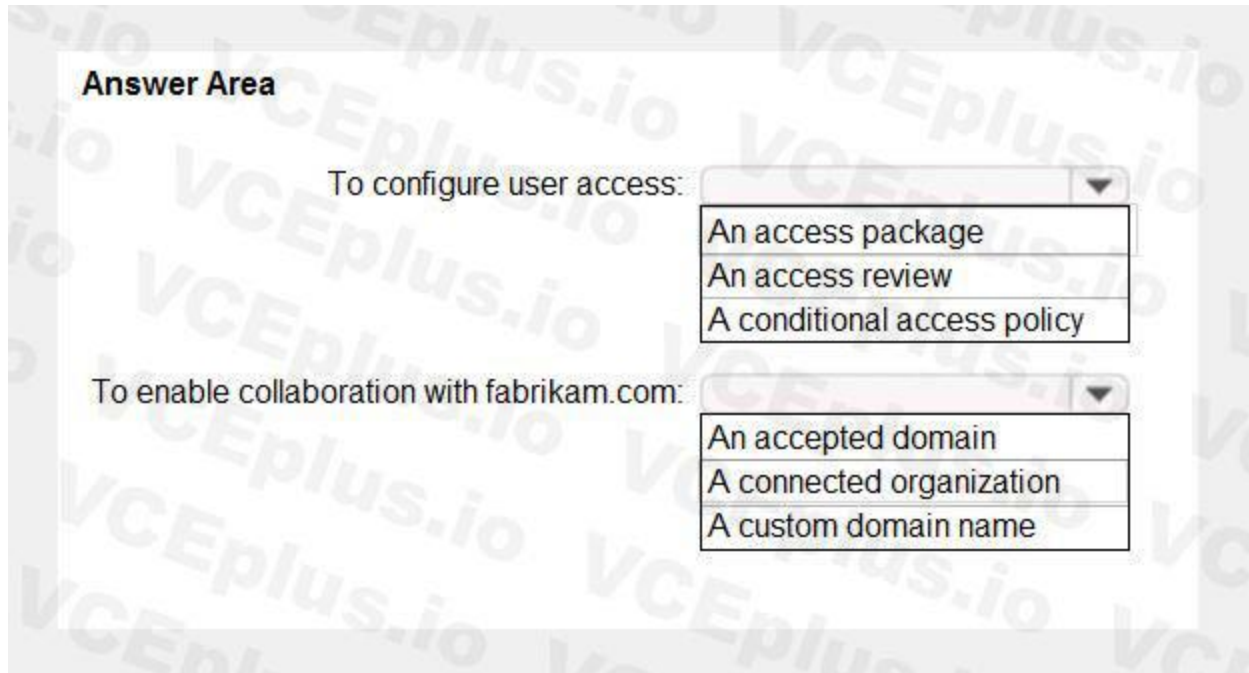
HOTSPOT

You need to implement the planned changes and technical requirements for the marketing department.

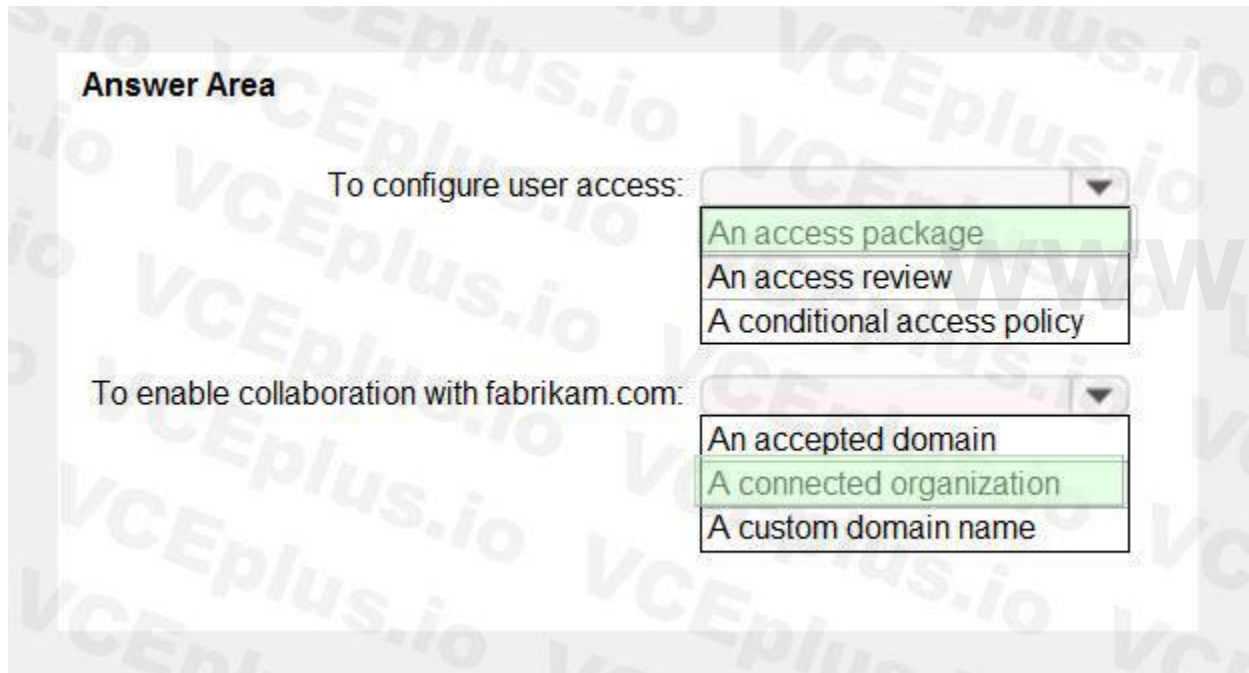
What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Hot Area:**



**Answer Area:**



**Section:**

**Explanation:**

Reference:

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

#### QUESTION 9

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:**

**Exam A**

**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 Azure Active Directory (Azure AD) tenant that syncs to an Active Directory forest.

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

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

Solution: You configure conditional access policies.

Does this meet the goal?

A. Yes

B. No

**Correct Answer: B**

**Section:**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn>

**QUESTION 2**

You have an Azure Active Directory (Azure AD) tenant that contains a user named SecAdmin1.

SecAdmin1 is assigned the Security administrator role.

SecAdmin1 reports that she cannot reset passwords from the Azure AD Identity Protection portal.

You need to ensure that SecAdmin1 can manage passwords and invalidate sessions on behalf of nonadministrative users. The solution must use the principle of least privilege.

Which role should you assign to SecAdmin1?

A. Authentication administrator

B. Helpdesk administrator

C. Privileged authentication administrator

D. Security operator

**Correct Answer: C**

**Section:**

**Explanation:**

Reference:

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

**QUESTION 3**

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



Custom smart lockout

Lockout threshold ⓘ

Lockout duration in seconds ⓘ

Custom banned passwords

Enforce custom list ⓘ ☒ Yes ☐ No

Custom banned password list ⓘ

- Contoso ✓
- Litware
- Tailwind
- project
- Zettabyte
- MainStreet

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ ☒ Yes ☐ No

Mode ⓘ ☒ Enforced ☐ Audit

You are evaluating the following passwords:

Pr0jectlitw@re

T@ilw1nd

C0nt0s0

Which passwords will be blocked?

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

**Correct Answer: C**

**Section:**

**Explanation:**

Reference:

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

#### QUESTION 4

You have a Microsoft 365 tenant.

All users have mobile phones and laptops.

The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity.

While working from the remote locations, the users connect their laptop to a wired network that has internet access.

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

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

- A. a verification code from the Microsoft Authenticator app

www.VCEplus.io

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

**Correct Answer: A**

**Section:**

**Explanation:**

#### QUESTION 5

You configure a new Microsoft 365 tenant to use a default domain name of contoso.com.

You need to ensure that you can control access to Microsoft 365 resources by using conditional access policies.

What should you do first?

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

**Correct Answer: B**

**Section:**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentalssecurity-defaults>

#### QUESTION 6

Your company recently implemented Azure Active Directory (Azure AD) Privileged Identity Management (PIM).

While you review the roles in PIM, you discover that all 15 users in the IT department at the company have permanent security administrator rights.

You need to ensure that the IT department users only have access to the Security administrator role when required.

What should you configure for the Security administrator role assignment?

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

**Correct Answer: D**

**Section:**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pimconfigure>

#### QUESTION 7

You have a Microsoft 365 tenant.

The Sign-ins activity report shows that an external contractor signed in to the Exchange admin center.

You need to review access to the Exchange admin center at the end of each month and block sign-ins if required.

What should you create?

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

**Correct Answer: C**

**Section:**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview>

#### QUESTION 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 Directory (Azure AD) and configure single sign-on (SSO) for MyApp1.

Which settings should you configure next for MyApp1?

- A. Self-service
- B. Provisioning
- C. 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 see 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. From 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 365 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 (MFA) registration policy1.
- D. Configure password protection for Windows Server Active Directory.

**Correct Answer: B**

**Section:**

#### QUESTION 13

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 14

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 15

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 16

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**

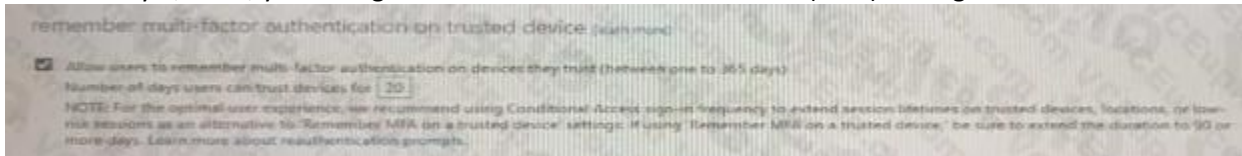
**Section:**

#### QUESTION 17

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.



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

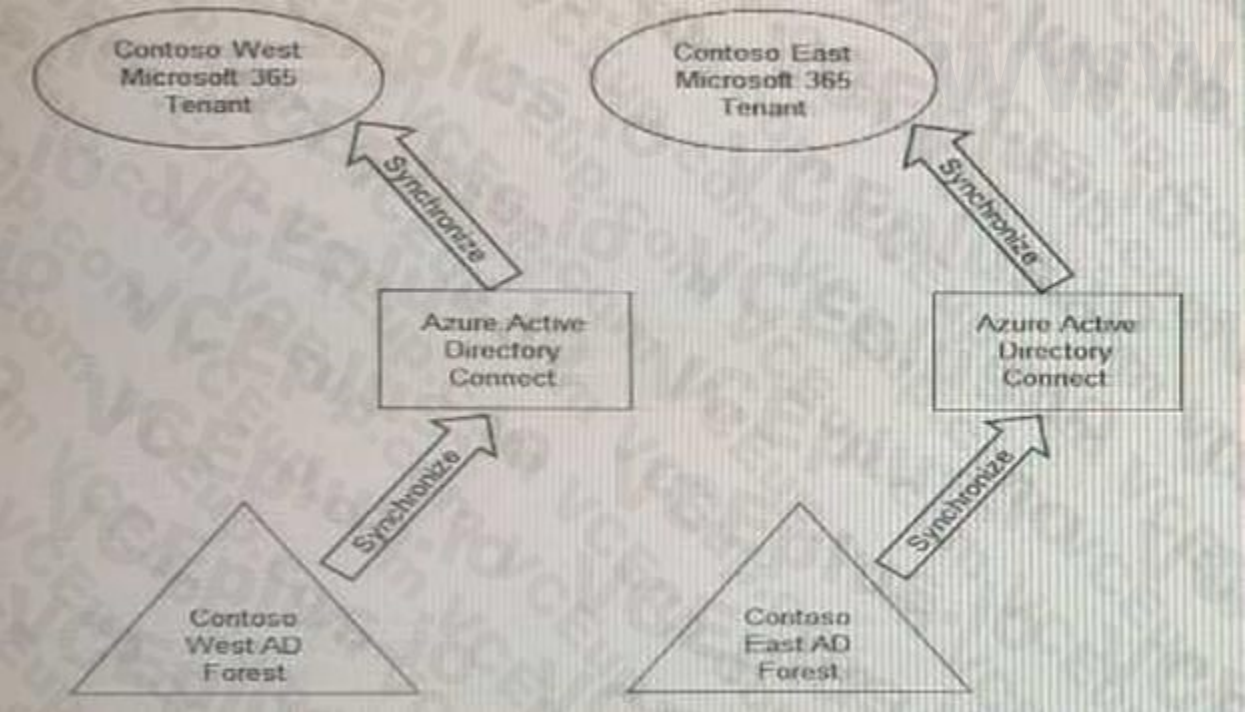
D.

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

**Correct Answer: B**  
**Section:**

**QUESTION 18**

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



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

- A. Configure 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.

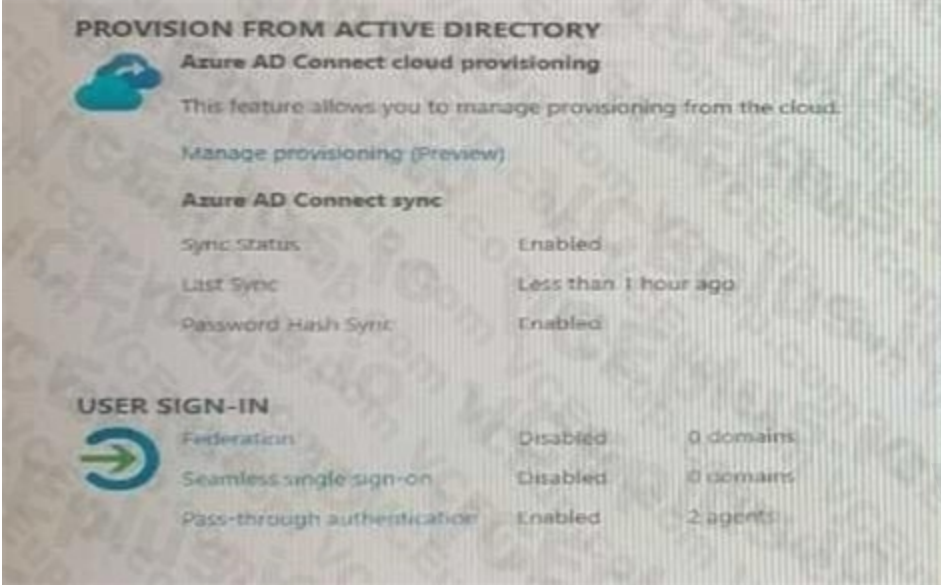
Correct Answer: D  
Section:

QUESTION 19

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.



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 20

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

- A. an access review
- B. the terms of 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 21

You have an Azure Active Directory (Azure AD) 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, Group4, and Group5

The groups are configured as shown in the following table.

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

www.VCEplus.io

**Correct Answer: B**

**Section:**

**Explanation:**

Reference:

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

#### QUESTION 22

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 23**

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 24**

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

- A. Yes
- B. No

www.VCEplus.io

**Correct Answer: B**

**Section:**

**QUESTION 25**

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

- A. Yes
- B. No

**Correct Answer: B**

**Section:**

**QUESTION 26**

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 27**

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 28**

**HOTSPOT**

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

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

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

NOTE: Each correct selection is worth one point.

**Hot Area:**

www.VCEplus.io

**Answer Area**

Job title property:

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

Usage location property:

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

**Answer Area:**

**Answer Area**

Job title property:

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

Usage location property:

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

**Section:**

**Explanation:**

#### QUESTION 29

You use Azure Monitor to analyze Azure Active Directory (Azure AD) activity logs.

You receive more than 100 email alerts each day for tailed Azure AD user sign-in attempts.

You need to ensure that a new security administrator receives the alerts instead of you.

Solution: From Azure monitor, you create a data collection rule.

Does this meet the goal?

A. Yes

B. No

**Correct Answer: B**

**Section:**

#### QUESTION 30

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 31

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 32

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 33

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 34

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.)

www.VCEplus.io

**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)

www.VCEplus.io

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@fabrikam.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 35**

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 36**

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

www.VCEplus.io

**Correct Answer: A, B****Section:****Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/external-identities/tutorial-bulk-invite>**QUESTION 37**

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 38

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 39

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 40

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

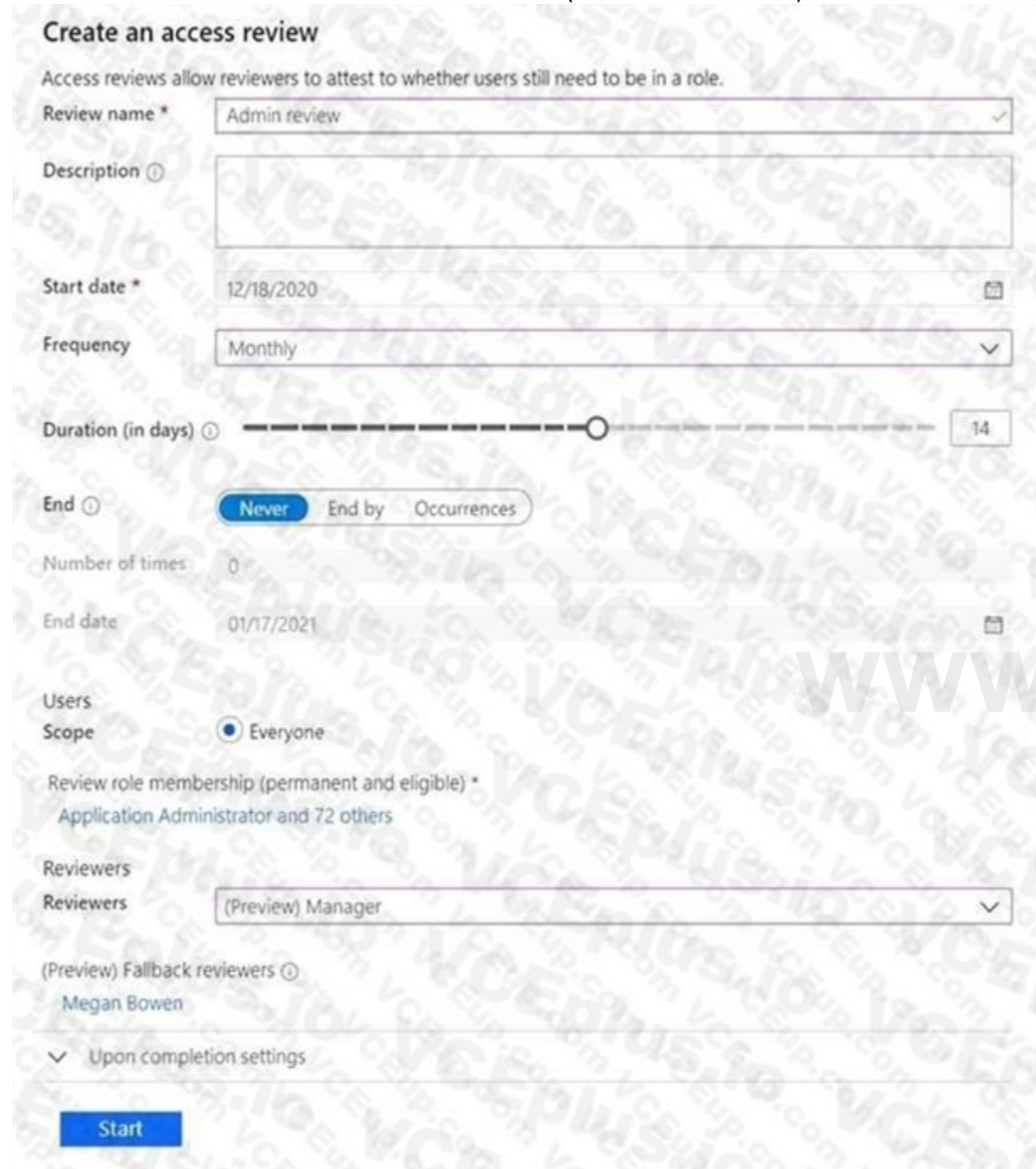
correct solution, while others might not have a correct solution.

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 (Preview) Manager

(Preview) Fallback reviewers Megan Bowen

Upon completion settings

**Start**

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

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

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

Does this meet the goal?

A. Yes

B. No

**Correct Answer: B**

**Section:**

**Explanation:**

Reference:

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

**QUESTION 41**

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 42

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.)

www.VCEplus.io



### Create an access review

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

Review name \*

Description

Start date \*

Frequency

Duration (in days)

End ☐ Never ☐ End by ☐ Occurrences

Number of times

End date

Users

Scope ☒ Everyone

Review role membership (permanent and eligible) \*

Application Administrator and 72 others

Reviewers

Reviewers

(Preview) Fallback reviewers

Upon completion settings

[Start](#)

www.VCEplus.io

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 43

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 44

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 45

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.

www.VCEplus.io

## 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 46

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

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

You have 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 47**

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 48**

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 49**

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

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

You have a Microsoft 365 tenant.

You have 100 IT administrators who are organized into 10 departments.

You create the access review shown in the exhibit. (Click the Exhibit tab.)

### Create an access review

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

Review name \* Admin review ✓

Description ⓘ

Start date \* 12/18/2020 📅

Frequency Monthly ▼

Duration (in days) ⓘ  14

End ⓘ Never End by Occurrences

Number of times 0

End date 01/17/2021 📅

Users Scope ☒ Everyone

Review role membership (permanent and eligible) \* Application Administrator and 72 others

Reviewers (Preview) Manager ▼

(Preview) Fallback reviewers ⓘ Megan Bowen

▼ Upon completion settings

**Start**

www.VCEplus.io

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 50**



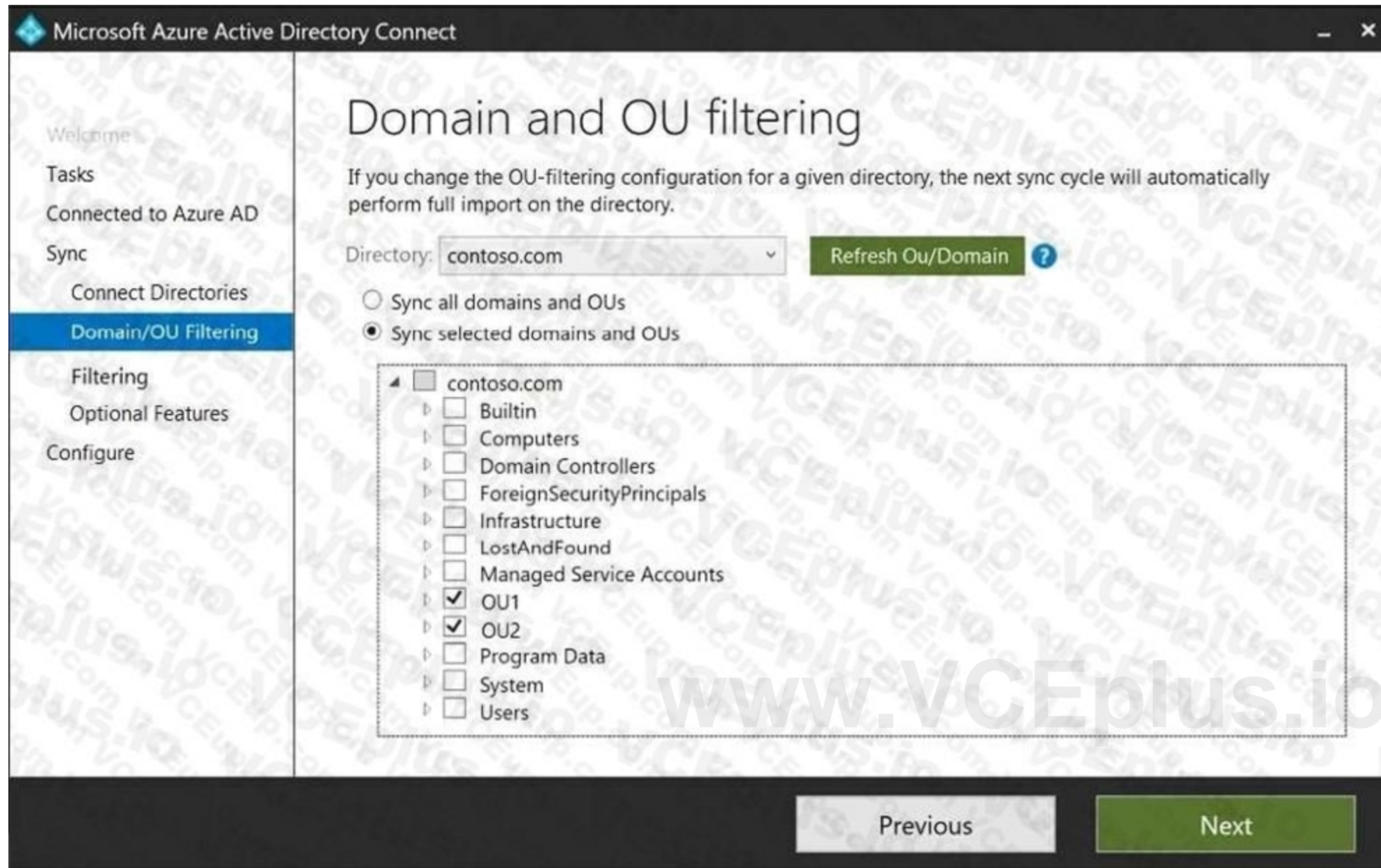
#### HOTSPOT

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

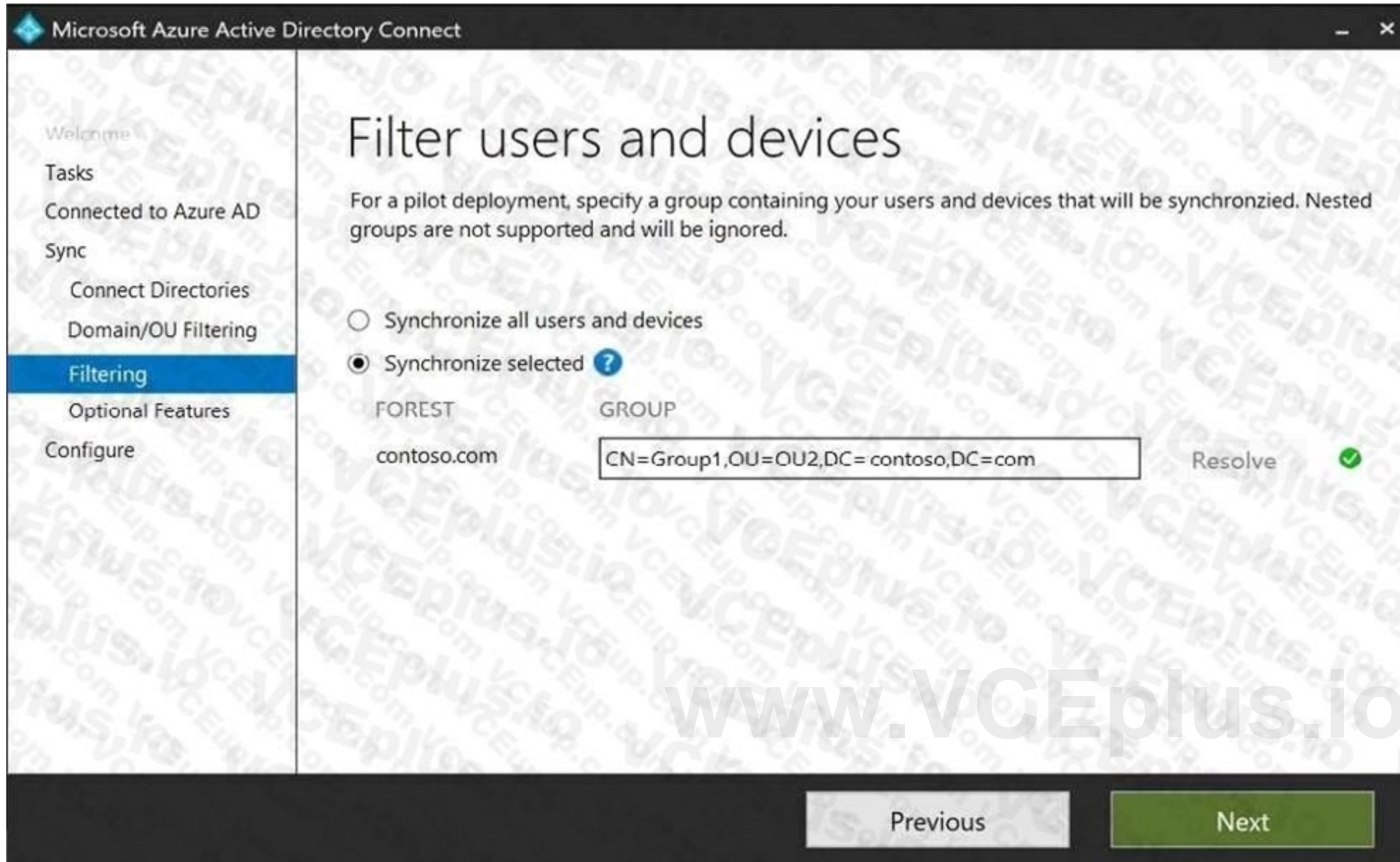
Name	Type	In organizational unit (OU)	Description
User1	User	OU1	User1 is a member of Group1.
User2	User	OU1	User2 is not a member of any groups.
Group1	Security group	OU2	User1 and Group2 are members of Group1.
Group2	Security group	OU1	Group2 is a member of Group1.

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.)

www.VCEplus.io



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



Microsoft Azure Active Directory Connect

Welcome

Tasks

Connected to Azure AD

Sync

Connect Directories

Domain/OU Filtering

**Filtering**

Optional Features

Configure

## Filter users and devices


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

☐ Synchronize all users and devices

☒ Synchronize selected ?

FOREST: contoso.com

GROUP: CN=Group1,OU=OU2,DC=contoso,DC=com

Resolve 

Previous Next

www.VCEplus.io

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.	<input type="radio"/>	<input type="radio"/>
User2 syncs to Azure AD.	<input type="radio"/>	<input type="radio"/>
Group2 syncs to Azure AD.	<input type="radio"/>	<input type="radio"/>

Answer Area:

Statements	Yes	No
User1 syncs to Azure AD.	<input checked="" type="radio"/>	<input type="radio"/>
User2 syncs to Azure AD.	<input type="radio"/>	<input checked="" type="radio"/>
Group2 syncs to Azure AD.	<input checked="" type="radio"/>	<input type="radio"/>

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 51

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 52

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

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

You have a Microsoft 365 tenant.

All users must use the Microsoft Authenticator app for multi-factor authentication (MFA) when accessing Microsoft 365 services.

Some users report that they received an MFA prompt on their Microsoft Authenticator app without initiating a sign-in request.

You need to block the users automatically when they report an MFA request that they did not initiate.

Solution: From the Azure portal, you configure the Notifications settings for multi-factor authentication (MFA).

Does this meet the goal?

- A. Yes
- B. No

**Correct Answer: B**

**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 53

HOTSPOT

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



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

In the tenant, you create the groups shown in the following table.

Name	Type	Membership type
GroupA	Security	Assigned
GroupB	Microsoft 365	Assigned

Which members can you add to GroupA and GroupB? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

GroupA:

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

GroupB:

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

Answer Area:

**Answer Area**

GroupA:

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

GroupB:

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

**Section:**

**Explanation:**

Reference:

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

#### QUESTION 54

DRAG DROP

You have a new Microsoft 365 tenant that uses a domain name of contoso.onmicrosoft.com.

You register the name contoso.com with a domain registrar.

You need to use contoso.com as the default domain name for new Microsoft 365 users.

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

**Select and Place:**

**Actions**

Delete the contoso.onmicrosoft.com domain.
Register a custom domain name of contoso.com.
Set the domain to primary.
Create a new TXT record in DNS.
Verify the domain name.

**Answer Area**

⏮

⏭

⏪

⏩

**Correct Answer:**

**Actions**

Delete the contoso.onmicrosoft.com domain.

**Answer Area**

Register a custom domain name of contoso.com.
Create a new TXT record in DNS.

⏮

⏭

⏪

⏩

**Section:**

**Explanation:**

Reference:

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

## QUESTION 55

HOTSPOT

You have a Microsoft 365 tenant named contoso.com.

Guest user access is enabled.


Users are invited to collaborate with contoso.com as shown in the following table.

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

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

Collaboration restrictions

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

 Delete

☒ TARGET DOMAINS

---

☐ Outlook.com

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

Hot Area:

Statements	Yes	No
User1 can accept the invitation and gain access to the enterprise application.	<input type="radio"/>	<input type="radio"/>
User2 can access the enterprise application.	<input type="radio"/>	<input type="radio"/>
User3 can accept the invitation and gain access to the SharePoint site.	<input type="radio"/>	<input type="radio"/>

Answer Area:



Statements	Yes	No
User1 can accept the invitation and gain access to the enterprise application.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can access the enterprise application.	<input checked="" type="radio"/>	<input type="radio"/>
User3 can accept the invitation and gain access to the SharePoint site.	<input type="radio"/>	<input checked="" type="radio"/>

**Section:**

**Explanation:**

Box 1: Yes

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

Box 2: Yes

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

Box 3: No

Invitations can only be sent to outlook.com. Therefore, User3 will not receive an invitation.

**QUESTION 56**

**DRAG DROP**

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

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

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

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

**Select and Place:**



### Actions

Sign in to the Microsoft 365 admin center.

Create a self-signed user account in the Azure AD tenant.

From the Microsoft 365 admin center, add the domain name.

Respond to the Become the admin message.

From the Microsoft 365 admin center, remove the domain name.

Create a TXT record in the contoso.com DNS zone.

### Answer Area



### Correct Answer:

### Actions

From the Microsoft 365 admin center, add the domain name.

From the Microsoft 365 admin center, remove the domain name.

### Answer Area

Create a self-signed user account in the Azure AD tenant.

Sign in to the Microsoft 365 admin center.

Respond to the Become the admin message.

Create a TXT record in the contoso.com DNS zone.



### Section:

### Explanation:

### Reference:

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

### QUESTION 57

### HOTSPOT

You have an Azure Active Directory (Azure AD) tenant that contains an administrative unit named Department1. Department1 has the users shown in the Users exhibit. (Click the Users tab.)

Dashboard > ContosoAzureAD > Department1 Administrative Unit

## Department1 Administrative Unit | Users (Preview)



ContosoAzureAD - Azure Active Directory

+ Add member | Remove member | Bulk operations | Refresh | Columns | Preview features | Got feedback?

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

Search users | Add filters

2 users found

Name	User principal name	User type	Directory synced
<input type="checkbox"/>  User1	User1@m365x629615.onmicrosoft.com	Member	No
<input type="checkbox"/>  User2	User2@m365x629615.onmicrosoft.com	Member	No

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



Dashboard > ContosoAzureAD > Department1 Administrative Unit

## Department1 Administrative Unit | Groups

ContosoAzureAD - Azure Active Directory

>> + Add | Remove | Refresh | Columns | Preview features | Got feedback?

Search groups | Add filters

Name	Group Type	Membership Type
<input type="checkbox"/>  Group1	Security	Assigned
<input type="checkbox"/>  Group2	Security	Assigned

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

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

## User Administrator | Assignments

Privileged Identity Management | Azure AD roles

» + Add assignments ⚙ Settings ↻ Refresh ↓ Export | ❤ Got feedback?

Eligible assignments Active assignments Expired assignments

🔍 Search by member name or principal name

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

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

Dashboard > ContosoAzureAD > Groups > Group2



## Group2 | Members

Group

» + Add members 🗑 Remove ↻ Refresh 📄 Bulk operations | 📄 Columns | 🖨 Preview features | ❤ Got feedback?

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

Direct members

Name	User type
<input type="checkbox"/>  User3	Member
<input type="checkbox"/>  User4	Member

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

Hot Area:



Statements	Yes	No
Admin1 can reset the passwords of User3 and User4.	<input type="radio"/>	<input type="radio"/>
Admin1 can add User1 to Group 2	<input type="radio"/>	<input type="radio"/>
Admin 2 can reset the password of User1.	<input type="radio"/>	<input type="radio"/>

Answer Area:

Statements	Yes	No
Admin1 can reset the passwords of User3 and User4.	<input type="radio"/>	<input checked="" type="radio"/>
Admin1 can add User1 to Group 2	<input type="radio"/>	<input checked="" type="radio"/>
Admin 2 can reset the password of User1.	<input checked="" type="radio"/>	<input type="radio"/>

Section:

Explanation:

Reference:

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

**QUESTION 58****HOTSPOT**

You have a Microsoft 365 tenant.

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

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

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

NOTE: Each correct selection is worth one point.

**Hot Area:**

**Answer Area**

Tool to use:

Azure AD Identity Protection
Identity Governance
Microsoft Cloud App Security
Microsoft Endpoint Manager

Policy type to create:

App discovery
App protection
Conditional access
OAuth app
Sign-in risk
User risk

**Answer Area:**



**Answer Area**

Tool to use:

- Azure AD Identity Protection
- Identity Governance
- Microsoft Cloud App Security
- Microsoft Endpoint Manager

Policy type to create:

- App discovery
- App protection
- Conditional access
- OAuth app
- Sign-in risk
- User risk

**Section:**

**Explanation:**

Reference:

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

#### QUESTION 59

HOTSPOT

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

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

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

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

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

NOTE: Each correct selection is worth one point.

**Hot Area:**

### Answer Area

Service to install on Server4:

- Azure AD Application Proxy
- The Azure AD Password Protection DC agent
- The Azure AD Password Protection proxy service
- Web Application Proxy in Windows Server

Rule to configure on Firewall1:

- Allow incoming HTTPS connections from Azure AD to Server4.
- Allow incoming IPsec connections from Azure AD to Server4.
- Allow outbound HTTPS connections from Server4 to Azure AD.
- Allow outbound IPsec connections from Server4 to Azure AD.

Answer Area:

### Answer Area

Service to install on Server4:

- Azure AD Application Proxy
- The Azure AD Password Protection DC agent
- The Azure AD Password Protection proxy service
- Web Application Proxy in Windows Server

Rule to configure on Firewall1:

- Allow incoming HTTPS connections from Azure AD to Server4.
- Allow incoming IPsec connections from Azure AD to Server4.
- Allow outbound HTTPS connections from Server4 to Azure AD.
- Allow outbound IPsec connections from Server4 to Azure AD.

Section:

Explanation:

Reference:

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

### QUESTION 60

HOTSPOT

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

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

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

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Can assign users to App1:

- Admin1 only
- Admin3 only
- Admin1 and Admin3 only
- Admin1, Admin2, and Admin3 only
- Admin1, Admin2, Admin3, and User1

Can register App2 in Azure AD:

- Admin1 only
- Admin3 only
- Admin1 and Admin3 only
- Admin1, Admin2, and Admin3 only
- Admin1, Admin2, Admin3, and User1

Answer Area:



**Answer Area**

Can assign users to App1:

Admin1 only
Admin3 only
Admin1 and Admin3 only
Admin1, Admin2, and Admin3 only
Admin1, Admin2, Admin3, and User1

Can register App2 in Azure AD:

Admin1 only
Admin3 only
Admin1 and Admin3 only
Admin1, Admin2, and Admin3 only
Admin1, Admin2, Admin3, and User1

**Section:**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/add-application-portal-assign-users>

<https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added>

#### QUESTION 61


HOTSPOT

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

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

### Role setting details - User Administrator

Privileged Identity Management | Azure AD roles

 Edit

---

#### Activation

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

#### Assignment

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

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

Hot Area:



### Answer Area

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

8 hours
15 days
1 month

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

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

### 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 62

### 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.	<input type="radio"/>	<input type="radio"/>
On December 11, 2020, User1 can accept Terms1 on Device2.	<input type="radio"/>	<input type="radio"/>
On December 7, 2020, User1 can accept Terms1 on Device3.	<input type="radio"/>	<input type="radio"/>

Answer Area:

Answer Area

Statements	Yes	No
On November 20, 2020, User1 can accept Terms1 on Device1.	<input checked="" type="radio"/>	<input type="radio"/>
On December 11, 2020, User1 can accept Terms1 on Device2.	<input checked="" type="radio"/>	<input type="radio"/>
On December 7, 2020, User1 can accept Terms1 on Device3.	<input type="radio"/>	<input checked="" type="radio"/>

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 63**

**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>

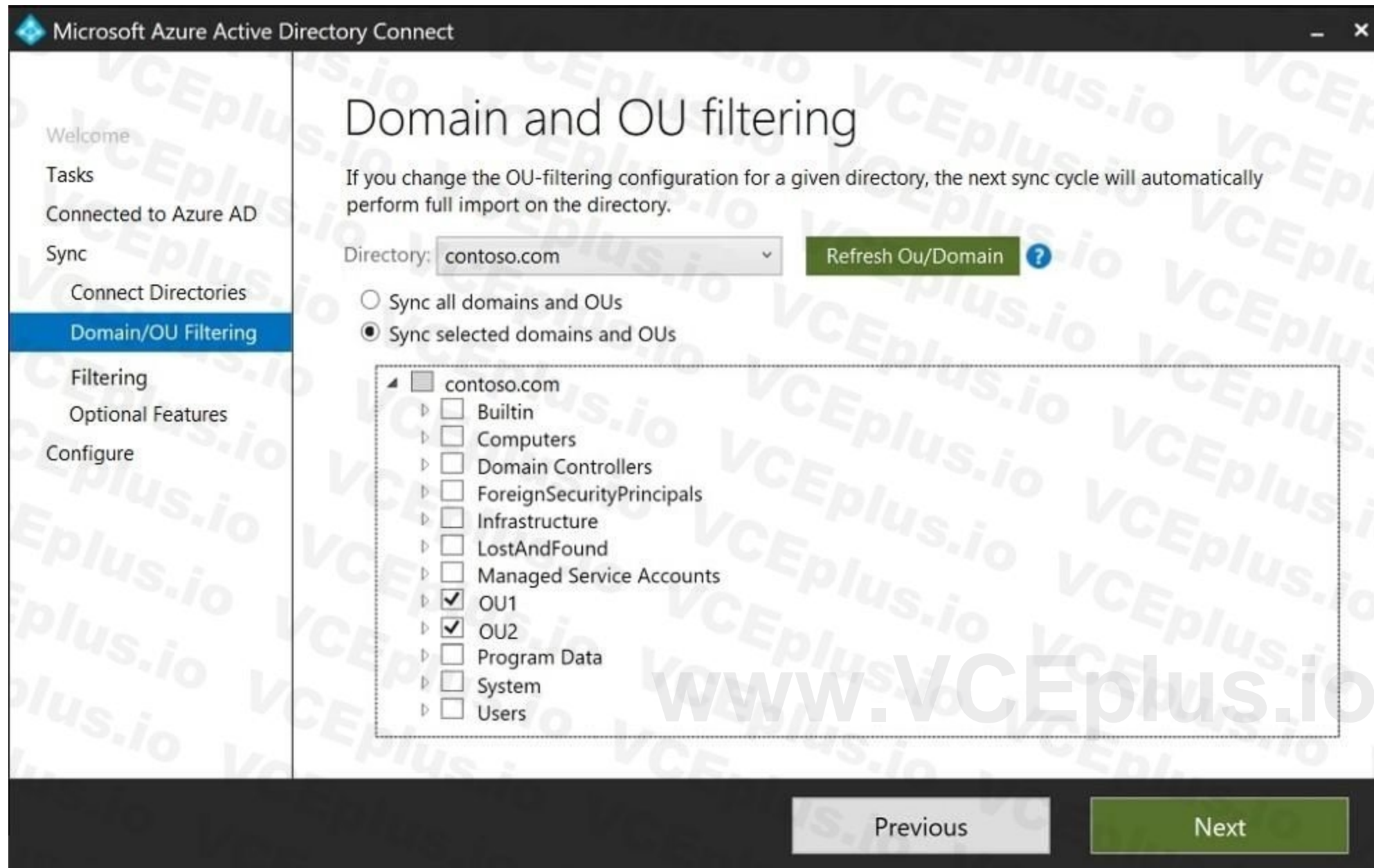
#### QUESTION 64

HOTSPOT

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

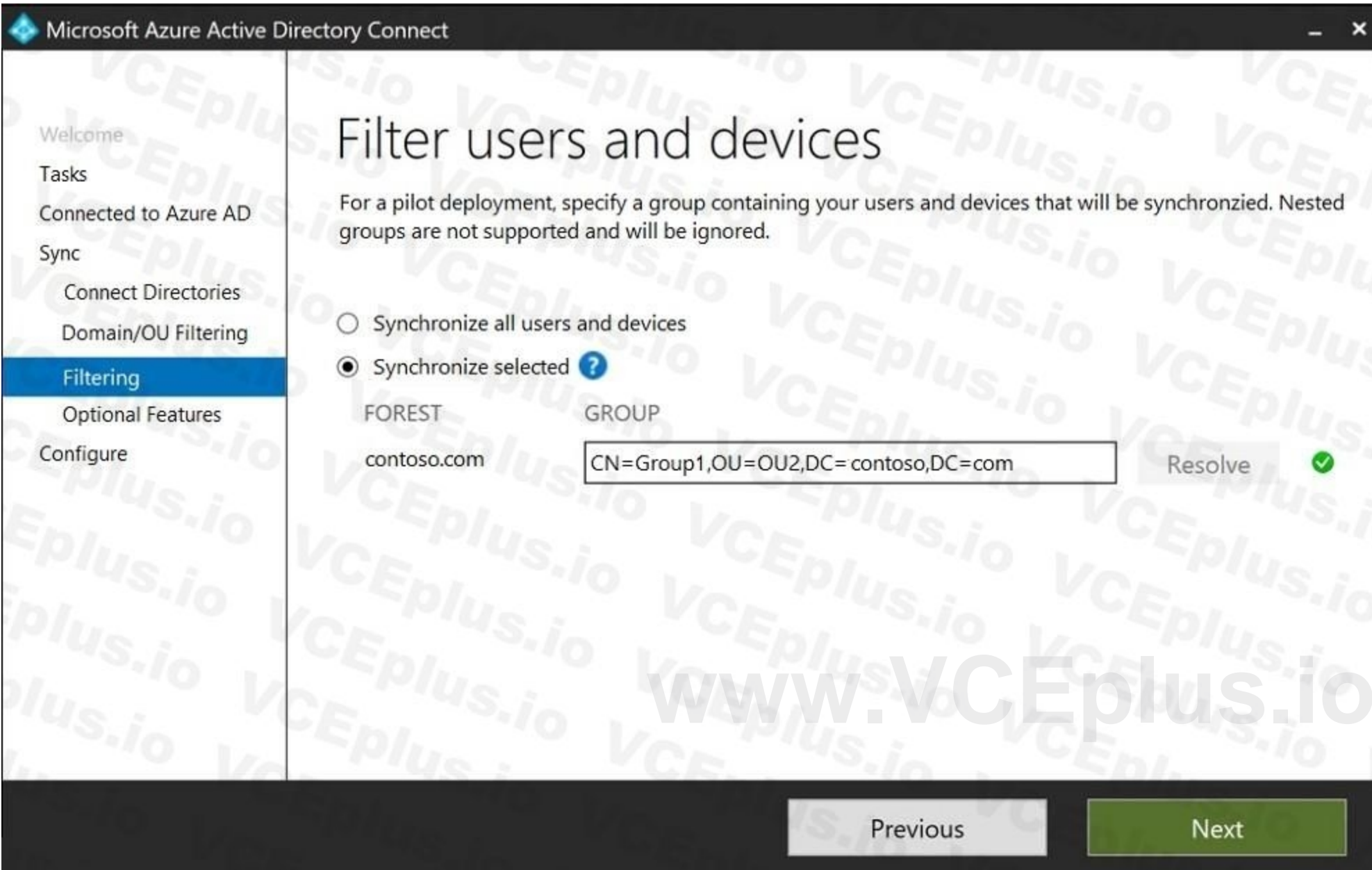
Name	Type	In organizational unit (OU)	Description
User1	User	OU1	User1 is a member of Group1.
User2	User	OU1	User2 is not a member of any groups.
Group1	Security group	OU2	User1 and Group2 are members of Group1.
Group2	Security group	OU1	Group2 is a member of Group1.

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



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





Microsoft Azure Active Directory Connect

Welcome

Tasks

Connected to Azure AD

Sync

Connect Directories

Domain/OU Filtering

**Filtering**

Optional Features

Configure

## Filter users and devices


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

☐ Synchronize all users and devices

☒ Synchronize selected ?

FOREST: contoso.com

GROUP: CN=Group1,OU=OU2,DC=contoso,DC=com

Resolve 

Previous Next

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

**Hot Area:**

Statements	Yes	No
User1 syncs to Azure AD.	<input type="radio"/>	<input type="radio"/>
User2 syncs to Azure AD.	<input type="radio"/>	<input type="radio"/>
Group2 syncs to Azure AD.	<input type="radio"/>	<input type="radio"/>

Answer Area:

Statements	Yes	No
User1 syncs to Azure AD.	<input checked="" type="radio"/>	<input type="radio"/>
User2 syncs to Azure AD.	<input type="radio"/>	<input checked="" type="radio"/>
Group2 syncs to Azure AD.	<input checked="" type="radio"/>	<input type="radio"/>

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 65

##### 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 66

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:

Role2:

Answer Area:

Answer Area

Role1:

Role2:

Section:

Explanation:

#### QUESTION 67

DRAG DROP

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

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

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

NOTE: Each correct selection is worth one point.

Select and Place:



Roles	Answer Area
Global administrator	User1: <input type="text"/> Role
Global reader	User2: <input type="text"/> Role
Reports reader	
Security operator	
Security reader	
User administrator	

Correct Answer:

Roles	Answer Area
<input type="text"/>	User1: <input type="text"/> Global administrator
Global reader	User2: <input type="text"/> Reports reader
<input type="text"/>	
Security operator	
Security reader	
User administrator	

Section:

Explanation:

QUESTION 68

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:

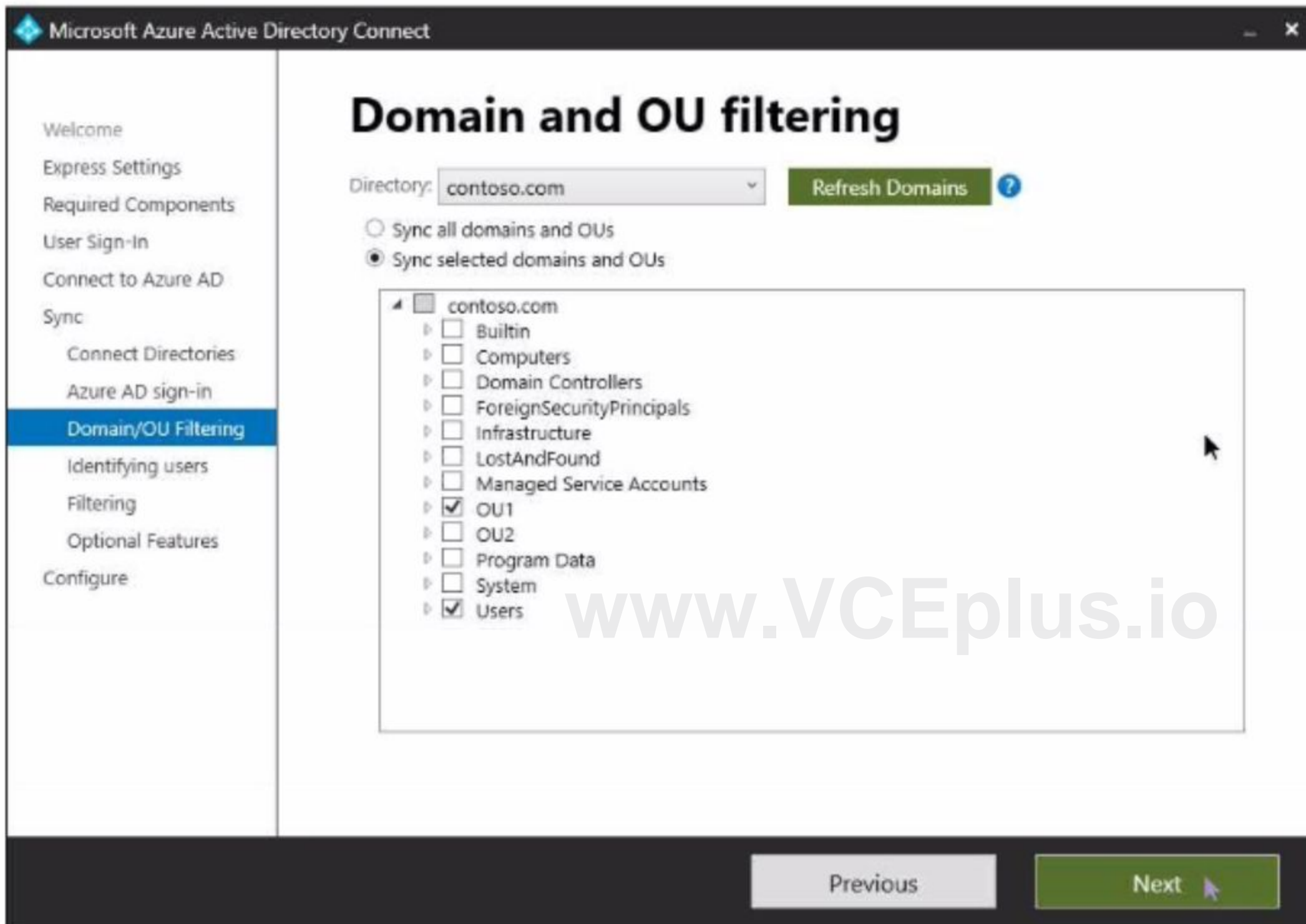
### QUESTION 69

HOTSPOT

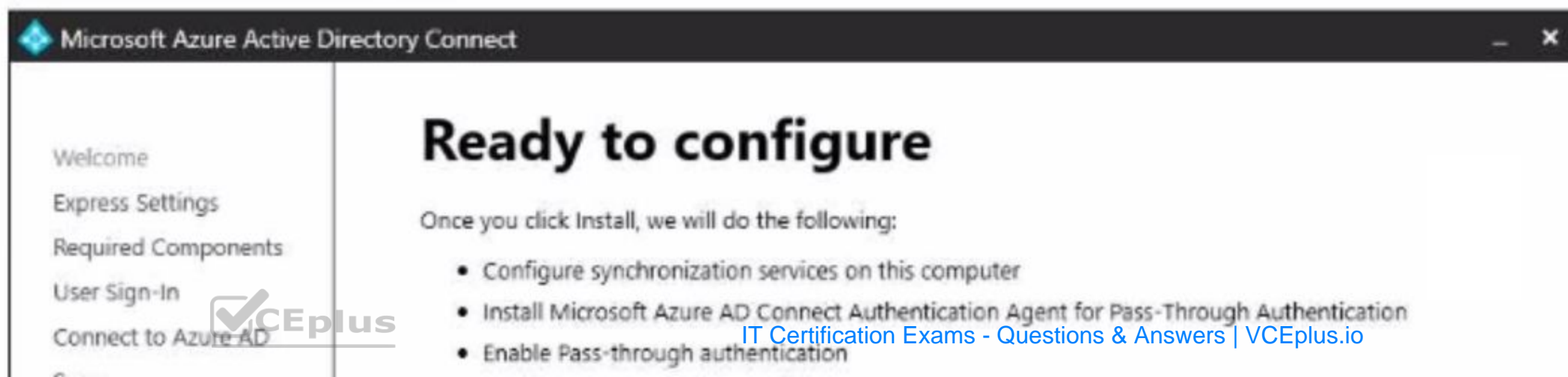
Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with Azure AD and contains the users shown in the following table.

Name	Organizational unit (OU)
User1	OU1
User2	OU2

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



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



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

Hot Area:

Answer Area

Statements

User1 can use self-service password reset (SSPR) to reset his password.

Yes

☐

No

☐

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

User1 can use self-service password reset (SSPR) to reset his password.

Yes

☒

No

☐

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 70

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 71**

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.)


[www.VCEplus.io](http://www.VCEplus.io)

## Create an access review

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

Review name \*  ✓

Description ⓘ

Start date \*  

Frequency  ✓

Duration (in days) ⓘ  14

End ⓘ ☐ Never ☒ End by ☐ Occurrences

Number of times

End date \*  

Users  
Users to review  ✓

Scope  
☐ Guest users only  
☒ Everyone

Group \*

Reviewers  
Reviewers  ✓

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.	<input type="radio"/>	<input type="radio"/>
On January 25, 2021, User2 can answer the Review1 question again.	<input type="radio"/>	<input type="radio"/>
On January 22, 2021, User3 can answer the Review1 question.	<input type="radio"/>	<input type="radio"/>

Answer Area:

Answer Area

Statements	Yes	No
On February 5, 2021, User1 can answer the Review1 question again.	<input checked="" type="radio"/>	<input type="radio"/>
On January 25, 2021, User2 can answer the Review1 question again.	<input checked="" type="radio"/>	<input type="radio"/>
On January 22, 2021, User3 can answer the Review1 question.	<input type="radio"/>	<input checked="" type="radio"/>

Section:



**Explanation:**

Reference:

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

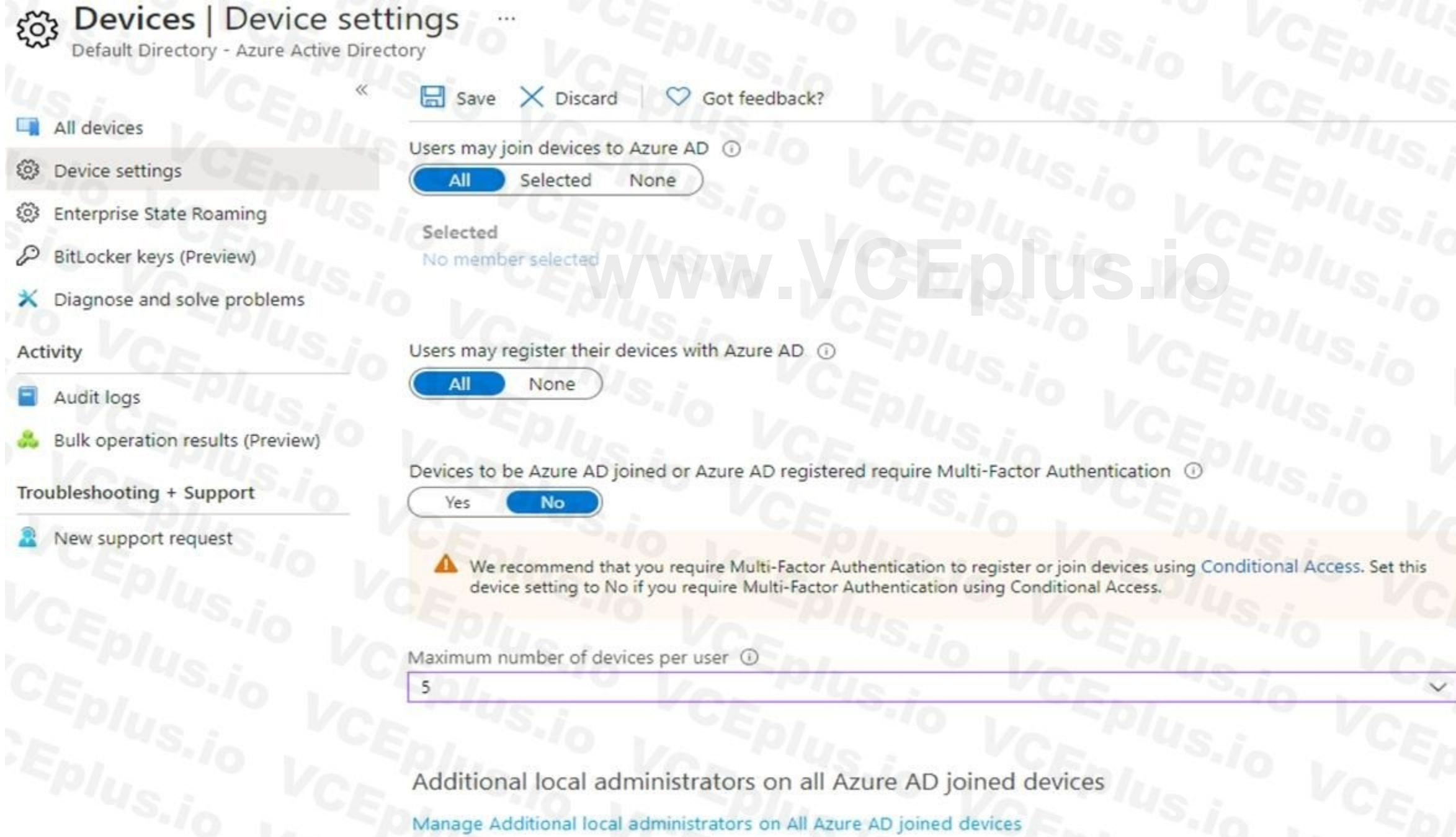
**QUESTION 72**

**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	<b>None</b>

You have the Device Settings shown in the following exhibit.



**Devices | Device settings** ...  
Default Directory - Azure Active Directory

« Save Discard Got feedback?

All devices

Device settings

Enterprise State Roaming

BitLocker keys (Preview)

Diagnose and solve problems

Activity

Audit logs

Bulk operation results (Preview)

Troubleshooting + Support

New support request

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.	<input type="radio"/>	<input type="radio"/>
	Admin1 can set Devices to be Azure AD joined or Azure AD registered require Multi-Factor Authentication to <b>Yes</b> .	<input type="radio"/>	<input type="radio"/>
	Admin2 is a local administrator on Device3.	<input type="radio"/>	<input type="radio"/>

Answer Area:

Answer Area	Statements	Yes	No
	User1 can join four additional Windows 10 devices to Azure AD.	<input checked="" type="radio"/>	<input type="radio"/>
	Admin1 can set Devices to be Azure AD joined or Azure AD registered require Multi-Factor Authentication to <b>Yes</b> .	<input type="radio"/>	<input checked="" type="radio"/>
	Admin2 is a local administrator on Device3.	<input type="radio"/>	<input checked="" type="radio"/>

Section:

Explanation:

Box 1: Yes

Users may join 5 devices to Azure AD.

Box 2: No

Cloud device administrator can 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 73

#### 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	<ul style="list-style-type: none"> <li>User administrator role</li> <li>Device Administrators role</li> <li>Identity Governance Administrator role</li> </ul>
User2	<ul style="list-style-type: none"> <li>Records Management role</li> <li>Quarantine Administrator role group</li> </ul>
User3	<ul style="list-style-type: none"> <li>Endpoint Security Manager role</li> <li>Intune Role Administrator role</li> </ul>

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
<input type="text"/>	
<input type="text"/>	User1: <input type="text" value="Azure Active Directory admin center"/>
<input type="text" value="Microsoft 365 compliance center"/>	User2: <input type="text" value="Exchange admin center"/>
<input type="text"/>	User3: <input type="text" value="Microsoft Endpoint Manager admin center"/>
<input type="text" value="SharePoint admin center"/>	

**Section:**

**Explanation:**

#### QUESTION 74

##### 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:**

www.VCEplus.io



**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 75

**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 76**

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:**

[www.VCEplus.io](http://www.VCEplus.io)