Exam Number:MS-500

Exam Name: Microsoft 365 Security Administration

Version: Demo

Testlet 1

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.
To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.
At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study
To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview
Fabrikam, Inc. is manufacturing company that sells products through partner retail stores. Fabrikam has 5,000 employees located in offices throughout Europe.

Existing Environment

Network Infrastructure
The network contains an Active Directory forest named fabrikam.com. Fabrikam has a hybrid Microsoft Azure Active Directory (Azure AD) environment.

The company maintains some on-premises servers for specific applications, but most end-user applications are provided by a Microsoft 365 E5 subscription.

Problem Statements
Fabrikam identifies the following issues:

Since last Friday, the IT team has been receiving automated email messages that contain "Unhealthy

Identity Synchronization Notification" in the subject line. Several users recently opened email attachments that contained malware. The process to remove the malware was time consuming.

Requirements

Planned Changes
Fabrikam plans to implement the following changes:

Fabrikam plans to monitor and investigate suspicious sign-ins to Active Directory

Fabrikam plans to provide partners with access to some of the data stored in Microsoft 365

Application Administration
Fabrikam identifies the following application requirements for managing workload applications:

User administrators will work from different countries

User administrators will use the Azure Active Directory admin center

Two new administrators named Admin1 and Admin2 will be responsible for managing Microsoft Exchange

Online only

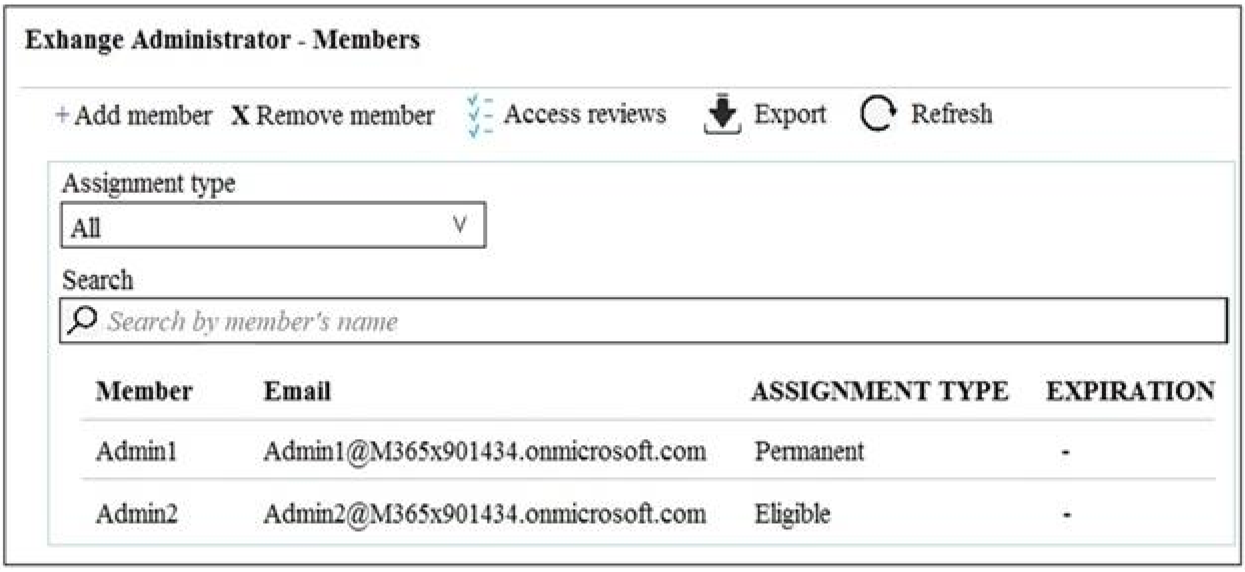
Security Requirements
Fabrikam identifies the following security requirements:

Access to the Azure Active Directory admin center by the user administrators must be reviewed every seven days. If an administrator fails to respond to an access request within three days, access must be removed
Users who manage Microsoft 365 workloads must only be allowed to perform administrative tasks for up to three hours at a time. Global administrators must be exempt from this requirement Users must be prevented from inviting external users to view company data. Only global administrators and a user named User1 must be able to send invitations
Azure Advanced Threat Protection (ATP) must capture security group modifications for sensitive groups, such as Domain Admins in Active Directory
Workload administrators must use multi-factor authentication (MFA) when signing in from an anonymous or an unfamiliar location
The location of the user administrators must be audited when the administrators authenticate to Azure AD

Email messages that include attachments containing malware must be delivered without the attachment

The principle of least privilege must be used whenever possible

Q1
An administrator configures Azure AD Privileged Identity Management as shown in the following exhibit.



Exhange Administrator - Members

Assignment type: All

Member	Email	ASSIGNMENT TYPE	EXPIRATION
Admin1	Admin1@M365x901434.onmicrosoft.com	Permanent	-
Admin2	Admin2@M365x901434.onmicrosoft.com	Eligible	-

What should you do to meet the security requirements?

A. Change the Assignment Type for Admin2 to Permanent
B. From the Azure Active Directory admin center, assign the Exchange administrator role to Admin2
C. From the Azure Active Directory admin center, remove the Exchange administrator role to Admin1
D. Change the Assignment Type for Admin1 to Eligible

Answer: D

Q2
You need to recommend a solution for the user administrators that meets the security requirements for auditing.

Which blade should you recommend using from the Azure Active Directory admin center?

A. Sign-ins

B. Azure AD Identity Protection
C. Authentication methods
D. Access review

Answer: A

References:
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins

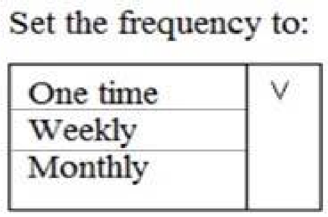
Q3
HOTSPOT

You plan to configure an access review to meet the security requirements for the workload administrators. You create an access review policy and specify the scope and a group.

Which other settings should you configure? To answer, select the appropriate options in the answer area.

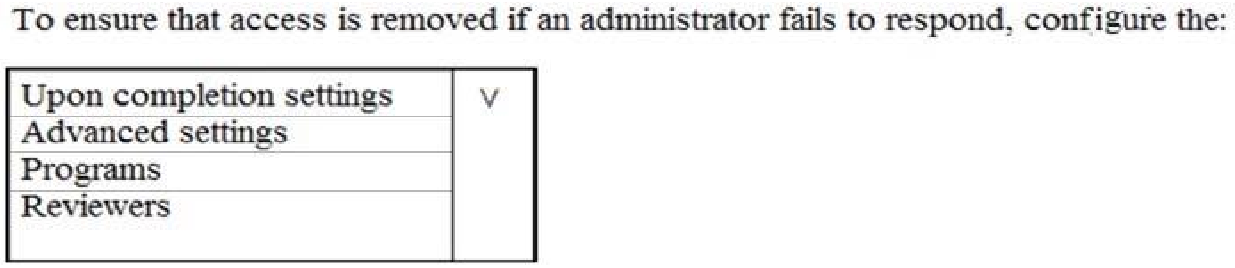
NOTE: Each correct selection is worth one point.

Hot Area:



Set the frequency to:

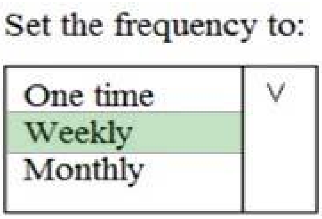
One time Weekly Monthly	V



To ensure that access is removed if an administrator fails to respond, configure the:

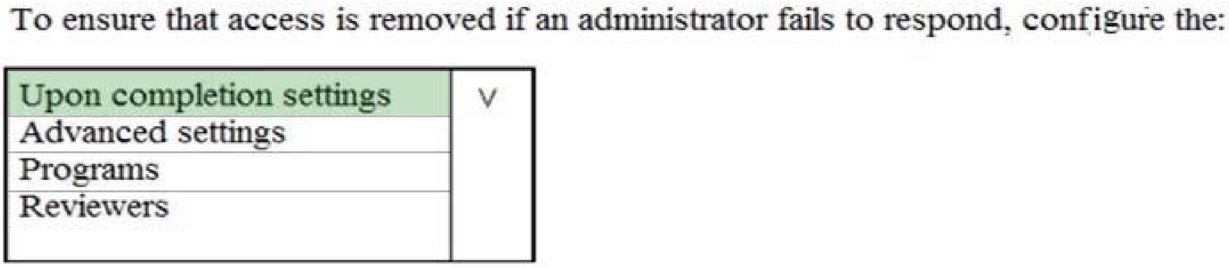
Upon completion settings Advanced settings Programs Reviewers	V

Answer:



Set the frequency to:

One time
[✓ Weekly]
Monthly



To ensure that access is removed if an administrator fails to respond, configure the:

[✓ Upon completion settings]
Advanced settings
Programs
Reviewers

Q4
You need to recommend a solution to protect the sign-ins of Admin1 and Admin2.

What should you include in the recommendation?

A. a device compliance policy
B. an access review
C. a user risk policy
D. a sign-in risk policy

Answer: C

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

Q5
You need to resolve the issue that generates the automated email messages to the IT team.

Which tool should you run first?

A. Synchronization Service Manager
B. Azure AD Connect wizard
C. Synchronization Rules Editor
D. IdFix

Answer: B

References:
https://docs.microsoft.com/en-us/office365/enterprise/fix-problems-with-directory-synchronization
Implement and manage identity and access

Testlet 2

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

Litware, Inc. is a financial company that has 1,000 users in its main office in Chicago and 100 users in a branch office in San Francisco.

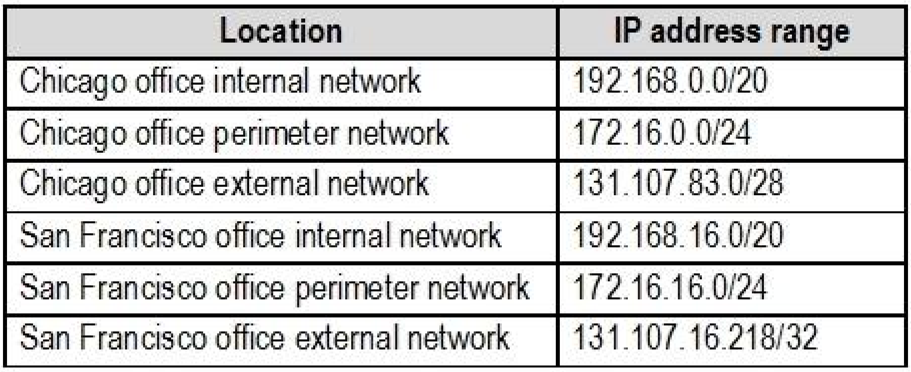
Existing Environment

Internal Network Infrastructure

The network contains a single domain forest. The forest functional level is Windows Server 2016.

Users are subject to sign-in hour restrictions as defined in Active Directory.

The network has the IP address ranges shown in the following table.



Location	IP address range
Chicago office internal network	192.168.0.0/20
Chicago office perimeter network	172.16.0.0/24
Chicago office external network	131.107.83.0/28
San Francisco office internal network	192.168.16.0/20
San Francisco office perimeter network	172.16.16.0/24
San Francisco office external network	131.107.16.218/32

The offices connect by using Multiprotocol Label Switching (MPLS).

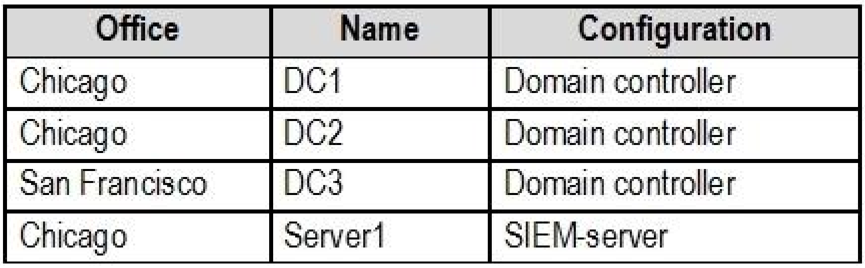
The following operating systems are used on the network:

Windows Server 2016

Windows 10 Enterprise

Windows 8.1 Enterprise

The internal network contains the systems shown in the following table.



Office	Name	Configuration
Chicago	DC1	Domain controller
Chicago	DC2	Domain controller
San Francisco	DC3	Domain controller
Chicago	Server1	SIEM-server

Litware uses a third-party email system.

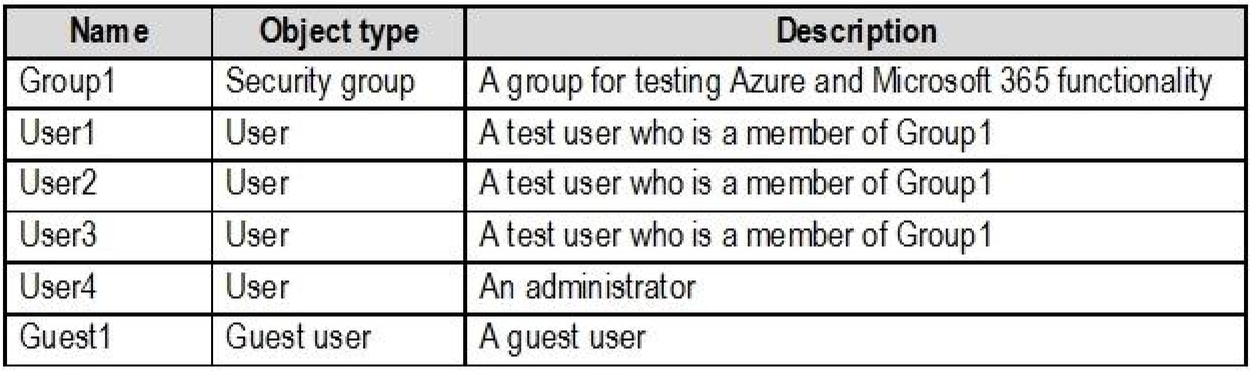
Cloud Infrastructure

Litware recently purchased Microsoft 365 subscription licenses for all users.

Microsoft Azure Active Directory (Azure AD) Connect is installed and uses the default authentication settings.

User accounts are not yet synced to Azure AD.

You have the Microsoft 365 users and groups shown in the following table.



Name	Object type	Description
Group1	Security group	A group for testing Azure and Microsoft 365 functionality
User1	User	A test user who is a member of Group1
User2	User	A test user who is a member of Group1
User3	User	A test user who is a member of Group1
User4	User	An administrator
Guest1	Guest user	A guest user

Requirements

Planned Changes

Litware plans to implement the following changes:

Migrate the email system to Microsoft Exchange Online

▪

Implement Azure AD Privileged Identity Management

▪

Security Requirements

Litware identifies the following security requirements:

Create a group named Group2 that will include all the Azure AD user accounts. Group2 will be used to provide limited access to Windows Analytics

Create a group named Group3 that will be used to apply Azure Information Protection policies to pilot users. Group3 must only contain user accounts

Use Azure Advanced Threat Protection (ATP) to detect any security threats that target the forest

▪

Prevent users locked out of Active Directory from signing in to Azure AD and Active Directory

▪

Implement a permanent eligible assignment of the Compliance administrator role for User1

▪

Configure domain-joined servers to ensure that they report sensor data to Microsoft Defender ATP

▪

Prevent access to Azure resources for the guest user accounts by default

▪

Ensure that all domain-joined computers are registered to Azure AD

▪

Multi-factor authentication (MFA) Requirements

Security features of Microsoft Office 365 and Azure will be tested by using pilot Azure user accounts.

You identify the following requirements for testing MFA:

Pilot users must use MFA unless they are signing in from the internal network of the Chicago office. MFA must NOT be used on the Chicago office internal network.

If an authentication attempt is suspicious, MFA must be used, regardless of the user location.

▪

Any disruption of legitimate authentication attempts must be minimized.

▪

General Requirements

Litware wants to minimize the deployment of additional servers and services in the Active Directory forest.

Q6

You need to create Group2.

What are two possible ways to create the group?

A. an Office 365 group in the Microsoft 365 admin center
B. a mail-enabled security group in the Microsoft 365 admin center
C. a security group in the Microsoft 365 admin center
D. a distribution list in the Microsoft 365 admin center
E. a security group in the Azure AD admin center

Answer: CE

Q7
Which IP address space should you include in the Trusted IP MFA configuration?

A. 131.107.83.0/28
B. 192.168.16.0/20
C. 172.16.0.0/24
D. 192.168.0.0/20

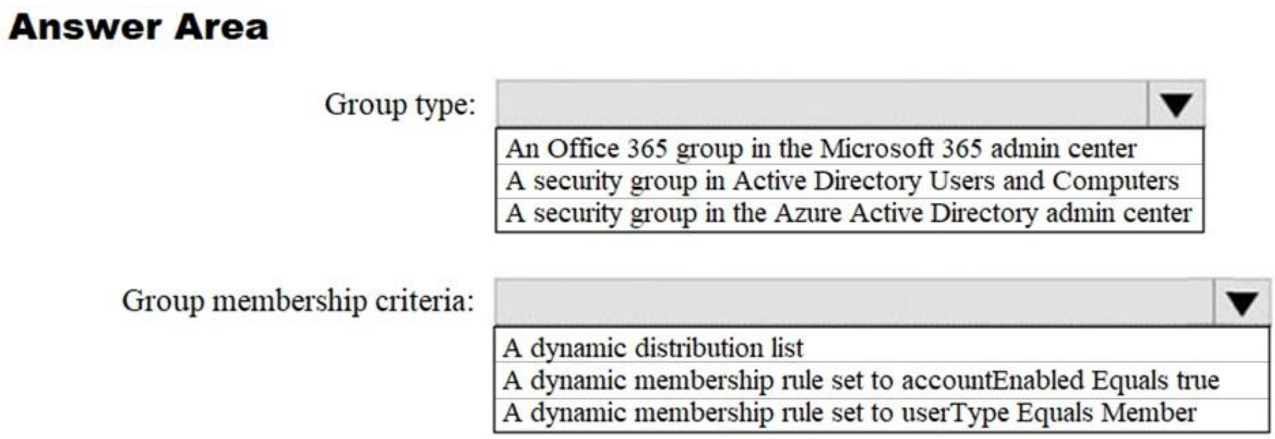
Answer: B

Q8
HOTSPOT

How should you configure Group3? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

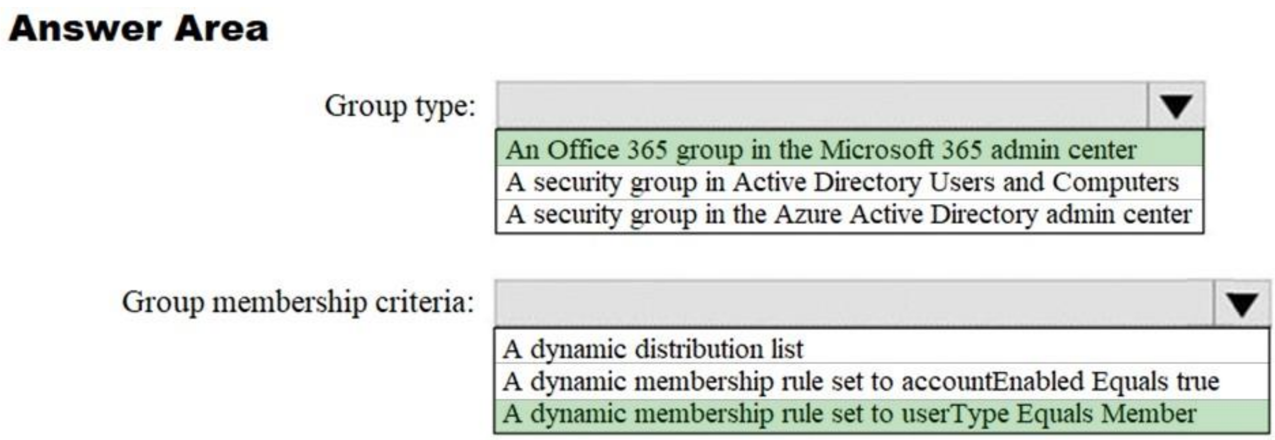
Group type:

- An Office 365 group in the Microsoft 365 admin center
- A security group in Active Directory Users and Computers
- A security group in the Azure Active Directory admin center

Group membership criteria:

- A dynamic distribution list
- A dynamic membership rule set to accountEnabled Equals true
- A dynamic membership rule set to userType Equals Member

Answer:



Answer Area

Group type: ▼

[✓ An Office 365 group in the Microsoft 365 admin center]
A security group in Active Directory Users and Computers
A security group in the Azure Active Directory admin center

Group membership criteria: ▼

A dynamic distribution list
A dynamic membership rule set to accountEnabled Equals true
[✓ A dynamic membership rule set to userType Equals Member]

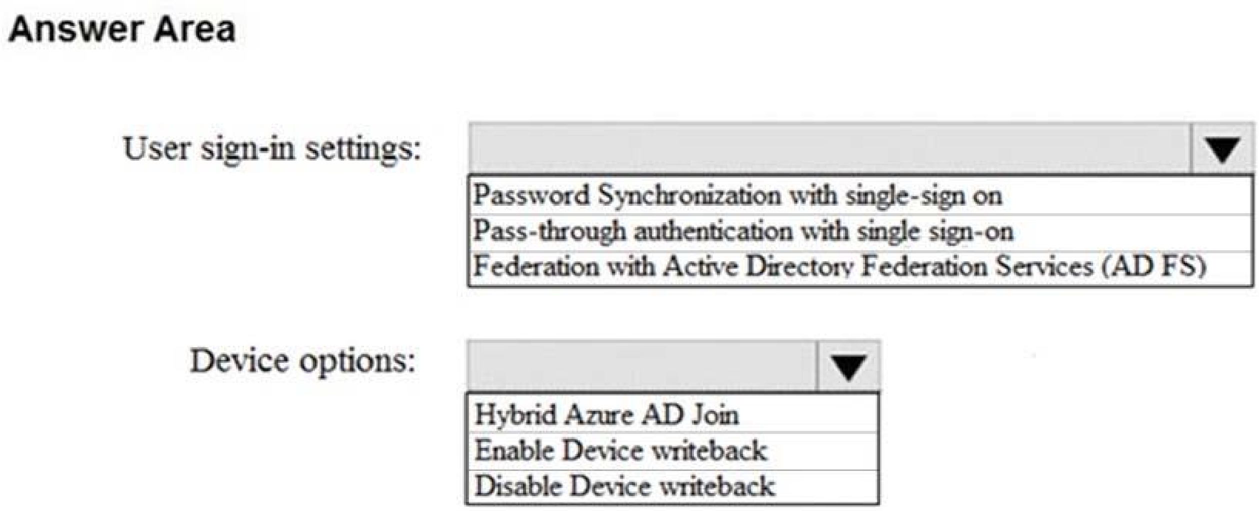
Reference:
https://docs.microsoft.com/en-us/azure/information-protection/prepare

Q9
HOTSPOT

How should you configure Azure AD Connect? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

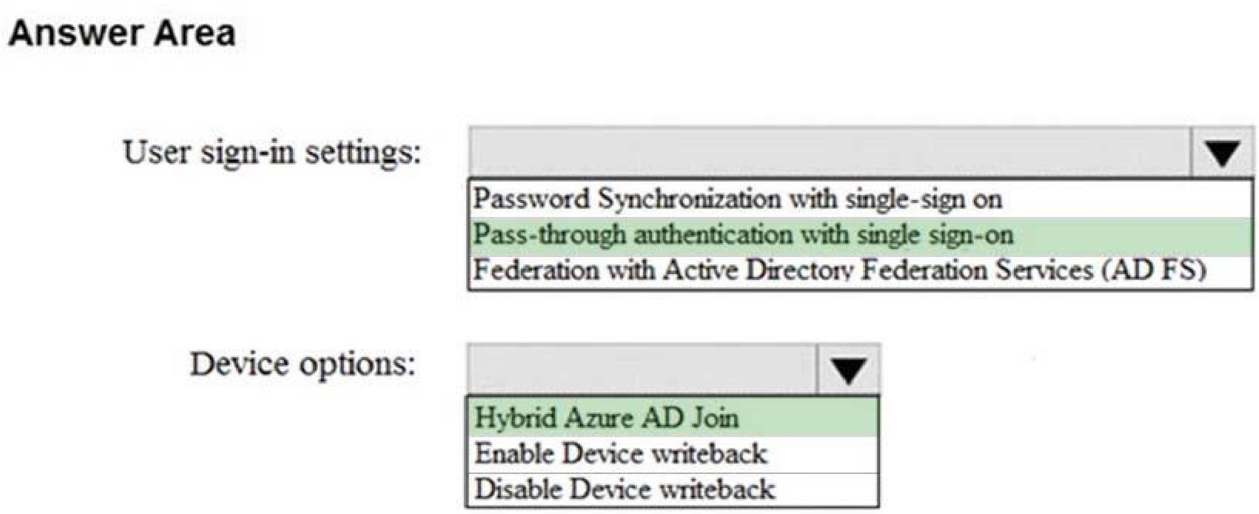
User sign-in settings: ▼

Password Synchronization with single-sign on
Pass-through authentication with single sign-on
Federation with Active Directory Federation Services (AD FS)

Device options: ▼

Hybrid Azure AD Join
Enable Device writeback
Disable Device writeback

Answer:



Answer Area

User sign-in settings:

- Password Synchronization with single-sign on
- Pass-through authentication with single sign-on
- Federation with Active Directory Federation Services (AD FS)

Device options:

- Hybrid Azure AD Join
- Enable Device writeback
- Disable Device writeback

Q10

You need to create Group3.

What are two possible ways to create the group?

A. an Office 365 group in the Microsoft 365 admin center

B. a mail-enabled security group in the Microsoft 365 admin center

C. a security group in the Microsoft 365 admin center

D. a distribution list in the Microsoft 365 admin center

E. a security group in the Azure AD admin center

Answer: AD

Testlet 3

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

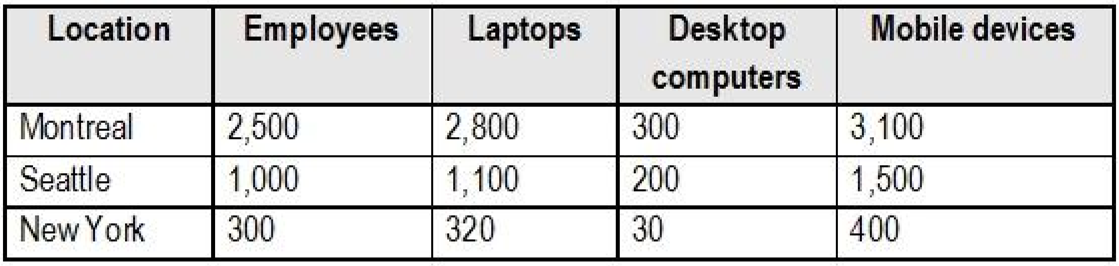
To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

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

The company has the offices shown in the following table.



Location	Employees	Laptops	Desktop computers	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

Contoso has IT, human resources (HR), legal, marketing, and finance departments. Contoso uses Microsoft 365.

Existing Environment

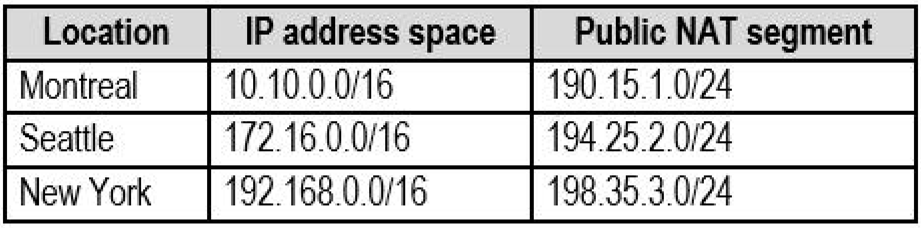
Infrastructure

The network contains an Active Directory domain named contoso.com that is synced to a Microsoft Azure Active Directory (Azure AD) tenant. Password writeback is enabled.

The domain contains servers that run Windows Server 2016. The domain contains laptops and desktop computers that run Windows 10 Enterprise.

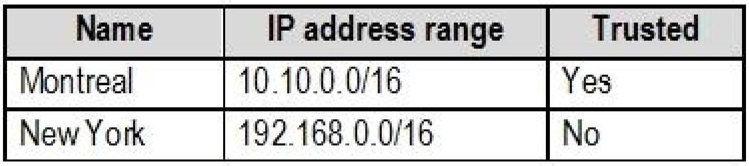
Each client computer has a single volume.

Each office connects to the Internet by using a NAT device. The offices have the IP addresses shown in the following table.



Location	IP address space	Public NAT segment
Montreal	10.10.0.0/16	190.15.1.0/24
Seattle	172.16.0.0/16	194.25.2.0/24
New York	192.168.0.0/16	198.35.3.0/24

Named locations are defined in Azure AD as shown in the following table.

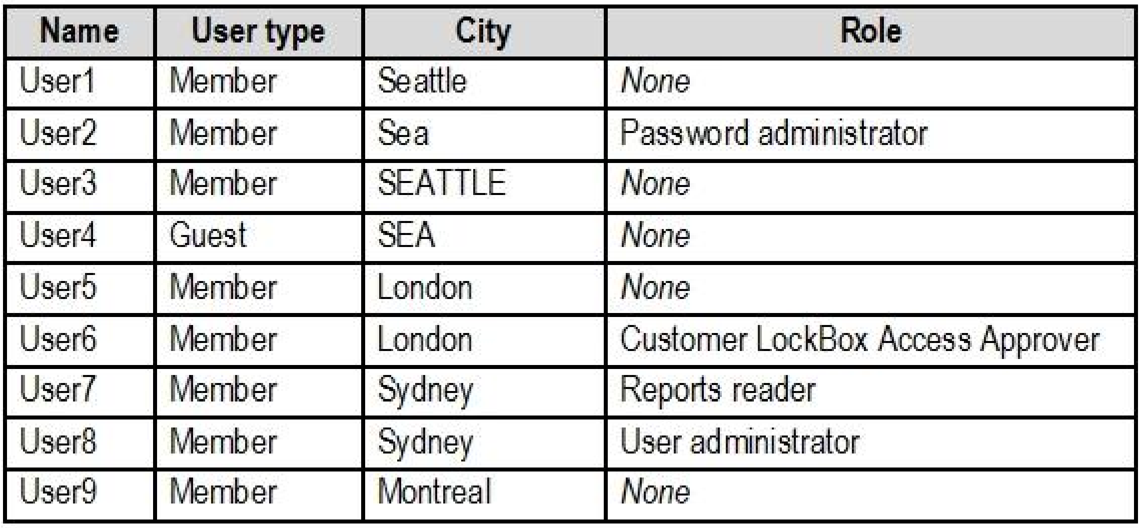


Name	IP address range	Trusted
Montreal	10.10.0.0/16	Yes
New York	192.168.0.0/16	No

From the Multi-Factor Authentication page, an address space of 198.35.3.0/24 is defined in the trusted IPs list.

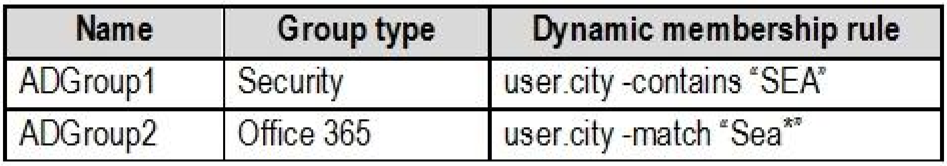
Azure Multi-Factor Authentication (MFA) is enabled for the users in the finance department.

The tenant contains the users shown in the following table.



Name	User type	City	Role
User1	Member	Seattle	*None*
User2	Member	Sea	Password administrator
User3	Member	SEATTLE	*None*
User4	Guest	SEA	*None*
User5	Member	London	*None*
User6	Member	London	Customer LockBox Access Approver
User7	Member	Sydney	Reports reader
User8	Member	Sydney	User administrator
User9	Member	Montreal	*None*

The tenant contains the groups shown in the following table.

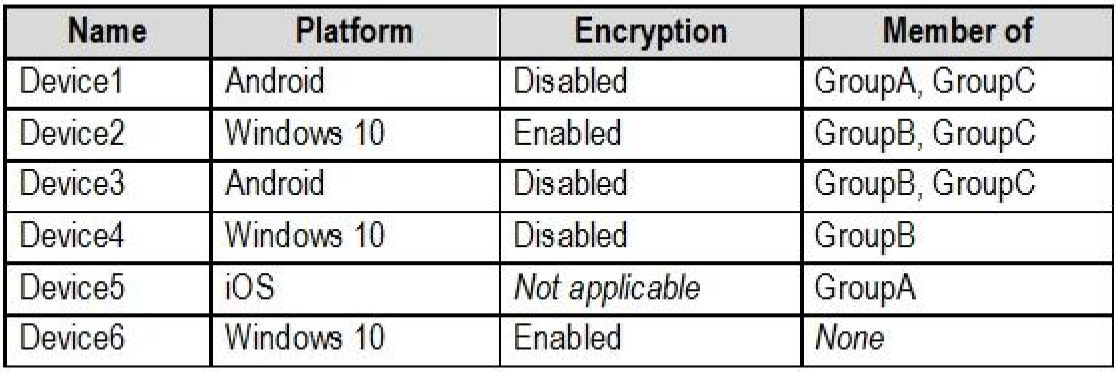


Name	Group type	Dynamic membership rule
ADGroup1	Security	user.city -contains “SEA”
ADGroup2	Office 365	user.city -match “Sea*”

Customer Lockbox is enabled in Microsoft 365.

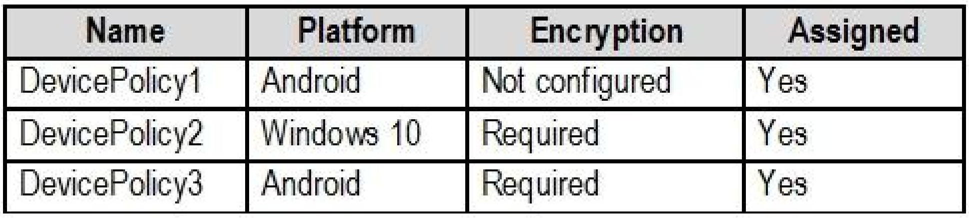
Microsoft Endpoint Manager Configuration

The devices enrolled in Microsoft Endpoint Manager are configured as shown in the following table.



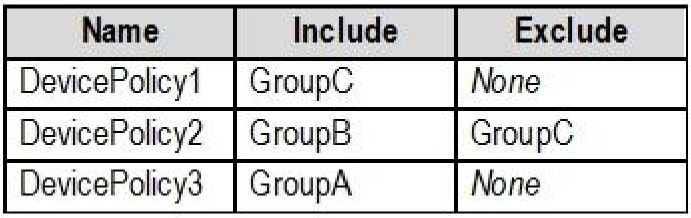
Name	Platform	Encryption	Member of
Device1	Android	Disabled	GroupA, GroupC
Device2	Windows 10	Enabled	GroupB, GroupC
Device3	Android	Disabled	GroupB, GroupC
Device4	Windows 10	Disabled	GroupB
Device5	iOS	*Not applicable*	GroupA
Device6	Windows 10	Enabled	*None*

The device compliance policies in Microsoft Endpoint Manager are configured as shown in the following table.



Name	Platform	Encryption	Assigned
DevicePolicy1	Android	Not configured	Yes
DevicePolicy2	Windows 10	Required	Yes
DevicePolicy3	Android	Required	Yes

The device compliance policies have the assignments shown in the following table.



Name	Include	Exclude
DevicePolicy1	GroupC	*None*
DevicePolicy2	GroupB	GroupC
DevicePolicy3	GroupA	*None*

The Mark devices with no compliance policy assigned as setting is set to Compliant.
Requirements
Technical Requirements
Contoso identifies the following technical requirements:
Use the principle of least privilege

▪

Enable User1 to assign the Reports reader role to users

▪

Ensure that User6 approves Customer Lockbox requests as quickly as possible

▪

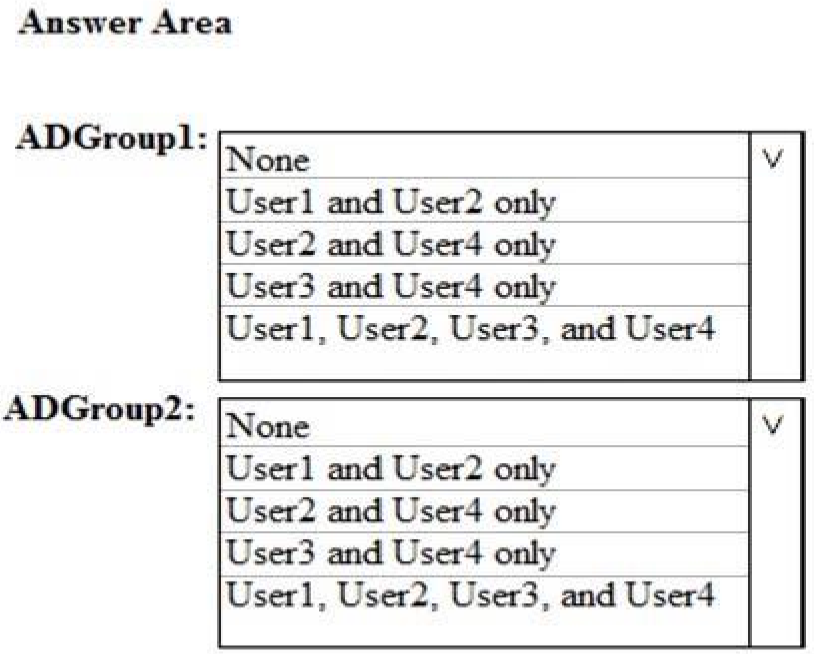
Ensure that User9 can enable and configure Azure AD Privileged Identity Management

Q11
HOTSPOT

Which users are members of ADGroup1 and ADGroup2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

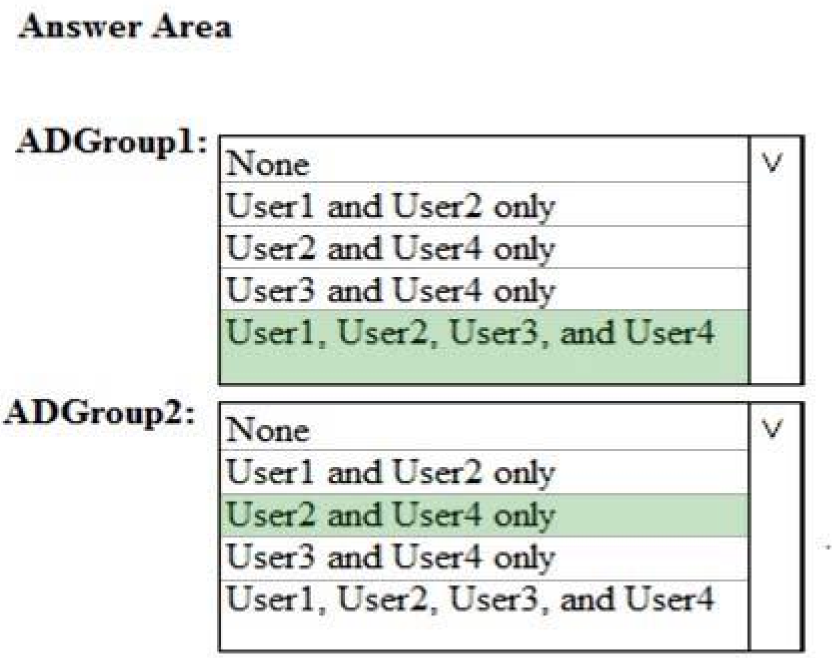
ADGroup1:

- None
- User1 and User2 only
- User2 and User4 only
- User3 and User4 only
- User1, User2, User3, and User4

ADGroup2:

- None
- User1 and User2 only
- User2 and User4 only
- User3 and User4 only
- User1, User2, User3, and User4

Answer:



Answer Area

ADGroup1:

- None
- User1 and User2 only
- User2 and User4 only
- User3 and User4 only
- [✓ User1, User2, User3, and User4]

ADGroup2:

- None
- User1 and User2 only
- [✓ User2 and User4 only]
- User3 and User4 only
- User1, User2, User3, and User4

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership#supported-values

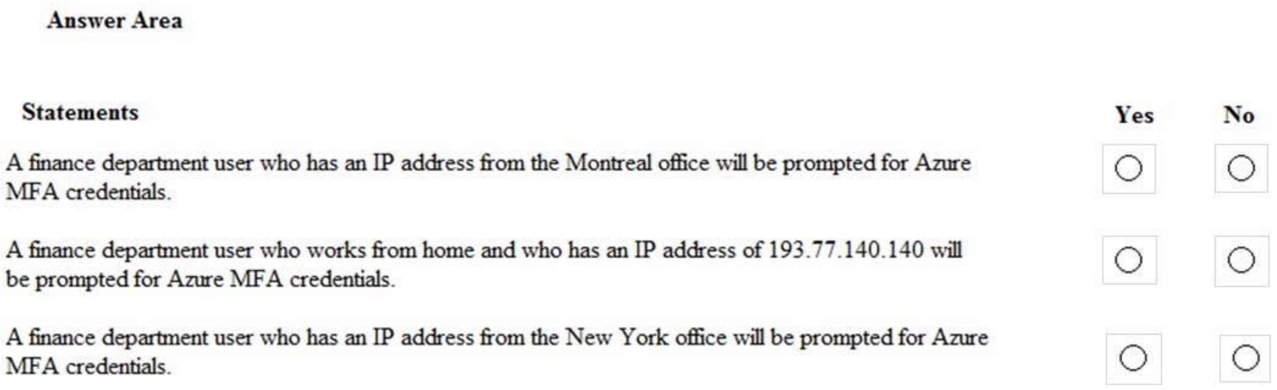
Q12
HOTSPOT

You are evaluating which finance department users will be prompted for Azure MFA credentials.

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

NOTE: Each correct selection is worth one point.

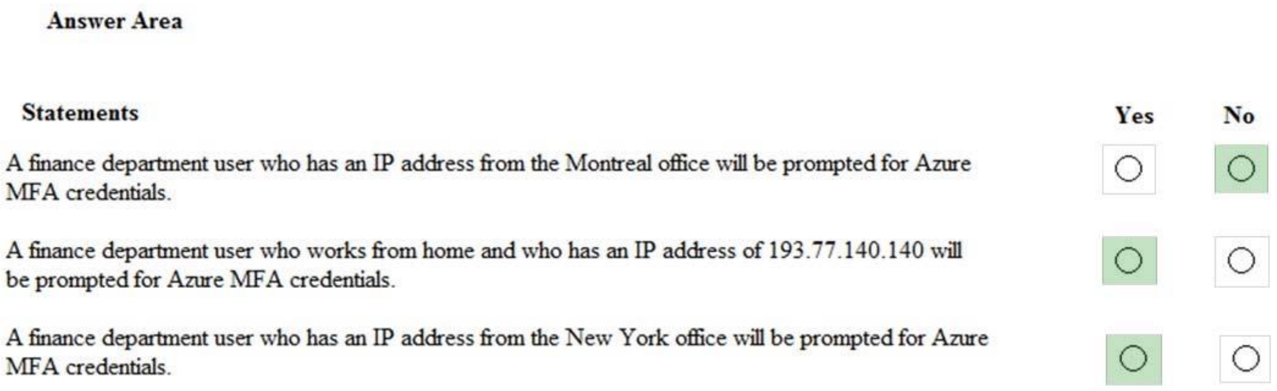
Hot Area:



Answer Area

Statements	Yes	No
A finance department user who has an IP address from the Montreal office will be prompted for Azure MFA credentials.	○	○
A finance department user who works from home and who has an IP address of 193.77.140.140 will be prompted for Azure MFA credentials.	○	○
A finance department user who has an IP address from the New York office will be prompted for Azure MFA credentials.	○	○

Answer:



Answer Area

Statements	Yes	No
A finance department user who has an IP address from the Montreal office will be prompted for Azure MFA credentials.	○	●
A finance department user who works from home and who has an IP address of 193.77.140.140 will be prompted for Azure MFA credentials.	●	○
A finance department user who has an IP address from the New York office will be prompted for Azure MFA credentials.	●	○

Q13

Which user passwords will User2 be prevented from resetting?

A. User6 and User7

B. User4 and User6

C. User4 only

D. User7 and User8

E. User8 only

Answer: C

Q14

You need to meet the technical requirements for User9. What should you do?

A. Assign the Privileged administrator role to User9 and configure a mobile phone number for User9
B. Assign the Compliance administrator role to User9 and configure a mobile phone number for User9
C. Assign the Security administrator role to User9
D. Assign the Global administrator role to User9

Answer: D

Q15
Which role should you assign to User1?

A. Global administrator
B. User administrator
C. Privileged role administrator
D. Security administrator

Answer: C

Question Set 4

Q16
You have a Microsoft 365 E5 subscription that is associated to a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

You use Active Directory Federation Services (AD FS) to federate on-premises Active Directory and the tenant. Azure AD Connect has the following settings:

Source Anchor: objectGUID

▪

Password Hash Synchronization: Disabled

▪

Password writeback: Disabled

▪

Directory extension attribute sync: Disabled

▪

Azure AD app and attribute filtering: Disabled

▪

Exchange hybrid deployment: Disabled

▪

User writeback: Disabled

▪

You need to ensure that you can use leaked credentials detection in Azure AD Identity Protection.

Solution: You modify the Azure AD app and attribute filtering settings.

Does that meet the goal?

A. Yes
B. No

Answer: B

Q17
You have a Microsoft 365 E5 subscription that is associated to a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

You use Active Directory Federation Services (AD FS) to federate on-premises Active Directory and the tenant. Azure AD Connect has the following settings:

Source Anchor: objectGUID

▪

Password Hash Synchronization: Disabled

▪

Password writeback: Disabled

▪

Directory extension attribute sync: Disabled

▪

Azure AD app and attribute filtering: Disabled

▪

Exchange hybrid deployment: Disabled

▪

User writeback: Disabled

▪

You need to ensure that you can use leaked credentials detection in Azure AD Identity Protection.

Solution: You modify the Password Hash Synchronization settings.

Does that meet the goal?

A. Yes
B. No

Answer: A

References:
https://docs.microsoft.com/en-us/azure/security/azure-ad-secure-steps

Q18
You have a Microsoft 365 E5 subscription that is associated to a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

You use Active Directory Federation Services (AD FS) to federate on-premises Active Directory and the tenant. Azure AD Connect has the following settings:

Source Anchor: objectGUID

▪

Password Hash Synchronization: Disabled

▪

Password writeback: Disabled

▪

Directory extension attribute sync: Disabled

▪

Azure AD app and attribute filtering: Disabled

▪

Exchange hybrid deployment: Disabled

▪

User writeback: Disabled

▪

You need to ensure that you can use leaked credentials detection in Azure AD Identity Protection.

Solution: You modify the Source Anchor settings.

Does that meet the goal?

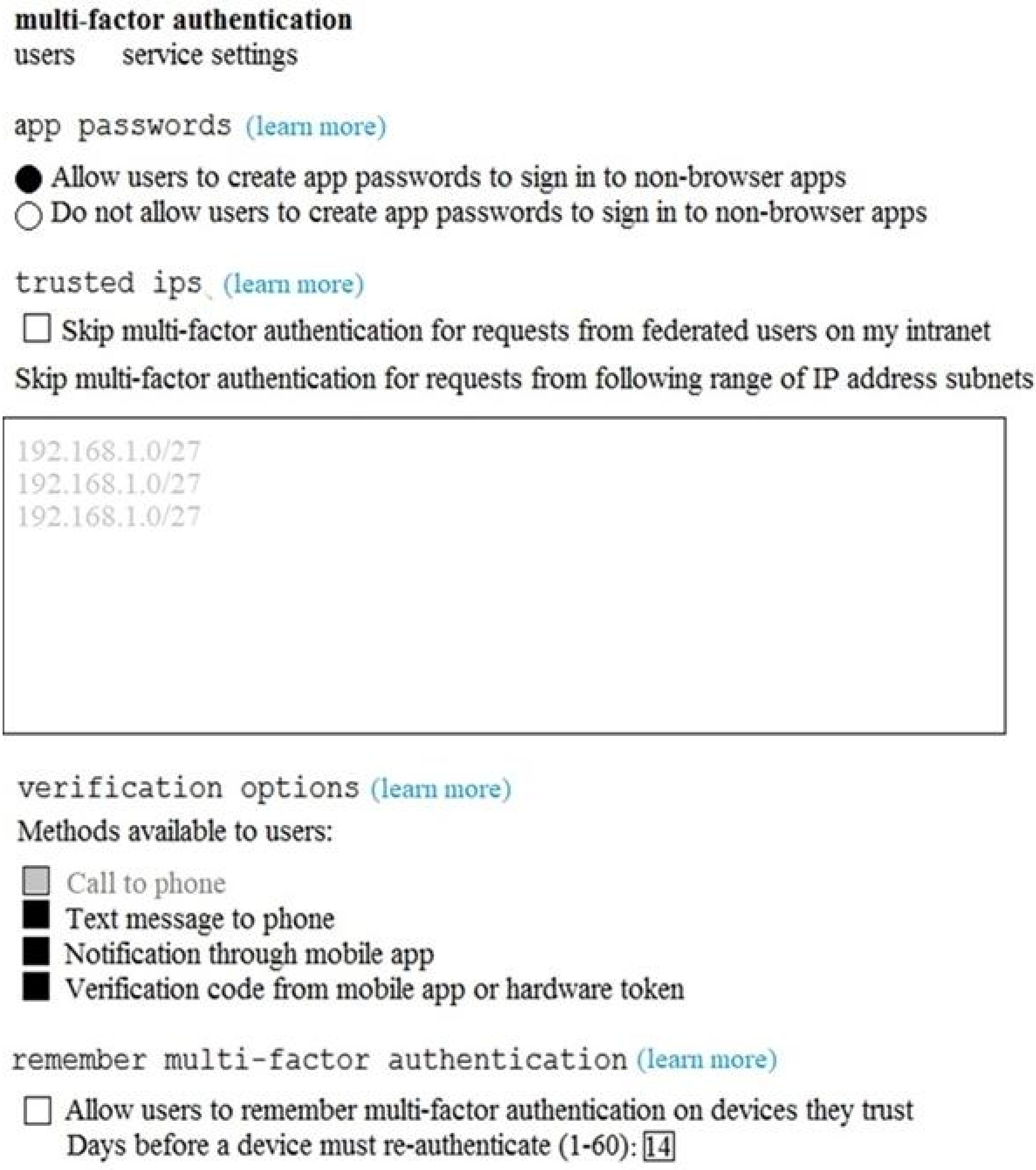
A. Yes
B. No

Answer: B

Q19
HOTSPOT

You have a Microsoft 365 subscription that uses a default domain name of contoso.com.

The multi-factor authentication (MFA) service settings are configured as shown in the exhibit. (Click the Exhibit tab.)



multi-factor authentication

users service settings

app passwords (learn more)

● Allow users to create app passwords to sign in to non-browser apps

○ Do not allow users to create app passwords to sign in to non-browser apps

trusted ips (learn more)

☐ Skip multi-factor authentication for requests from federated users on my intranet

Skip multi-factor authentication for requests from following range of IP address subnets

```
192.168.1.0/27
192.168.1.0/27
192.168.1.0/27
```

verification options (learn more)

Methods available to users:

☐ Call to phone

■ Text message to phone

■ Notification through mobile app

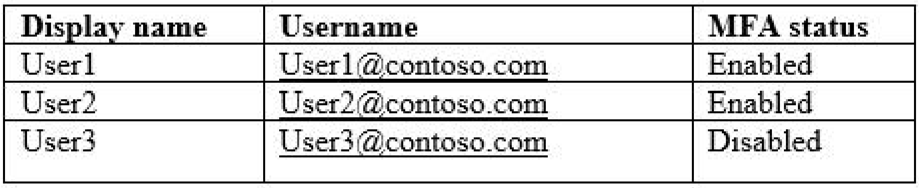
■ Verification code from mobile app or hardware token

remember multi-factor authentication (learn more)

☐ Allow users to remember multi-factor authentication on devices they trust

Days before a device must re-authenticate (1-60): 14

In contoso.com, you create the users shown in the following table.

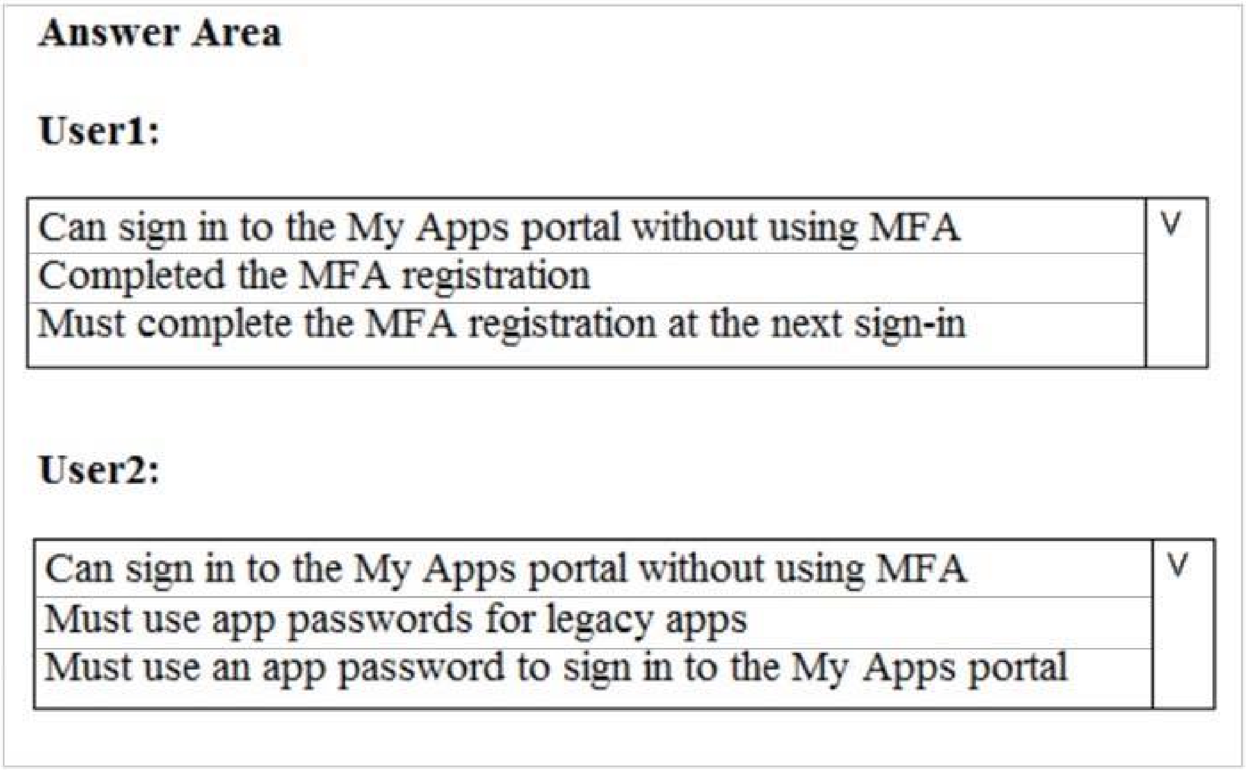


Display name	Username	MFA status
User1	User1@contoso.com	Enabled
User2	User2@contoso.com	Enabled
User3	User3@contoso.com	Disabled

What is the effect of the configuration? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

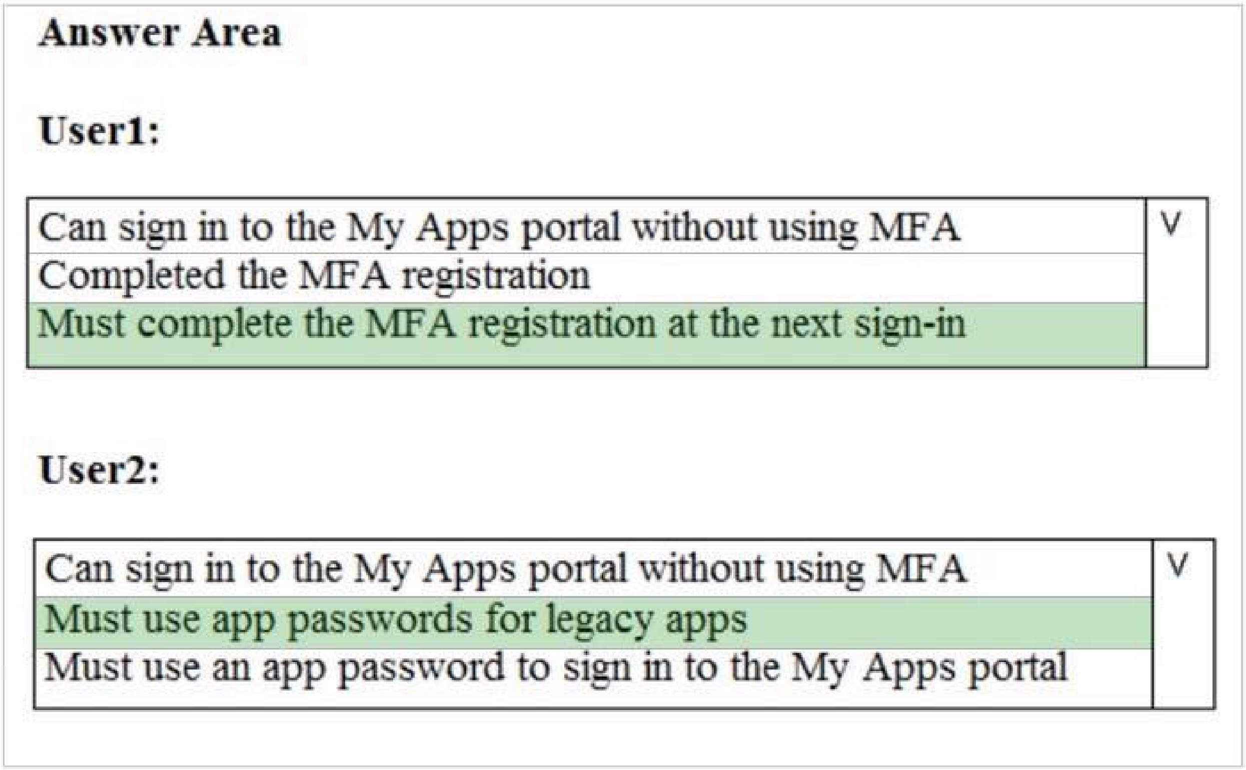
User1:

- Can sign in to the My Apps portal without using MFA
- Completed the MFA registration
- Must complete the MFA registration at the next sign-in

User2:

- Can sign in to the My Apps portal without using MFA
- Must use app passwords for legacy apps
- Must use an app password to sign in to the My Apps portal

Answer:



Answer Area

User1:

Can sign in to the My Apps portal without using MFA
Completed the MFA registration
[✓ Must complete the MFA registration at the next sign-in]

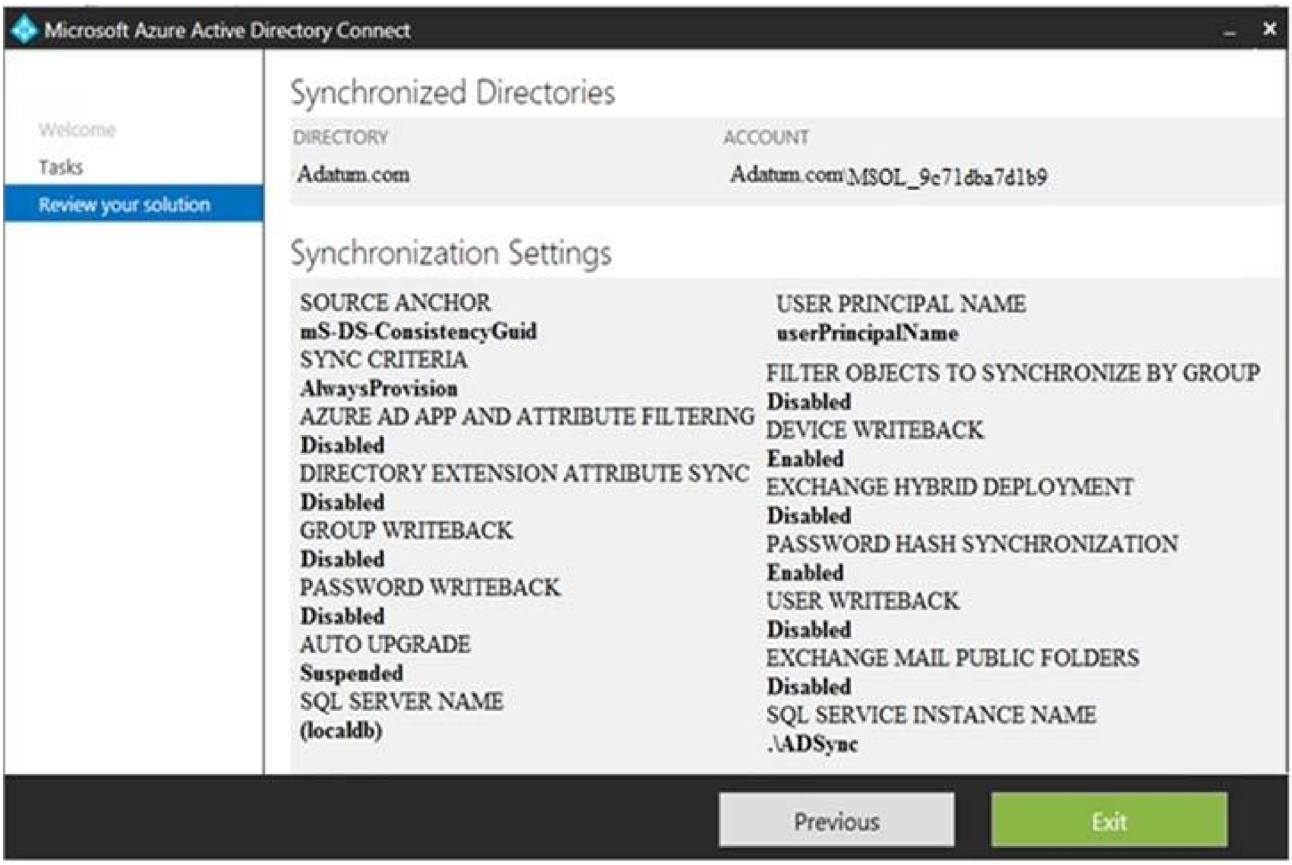
User2:

Can sign in to the My Apps portal without using MFA
[✓ Must use app passwords for legacy apps]
Must use an app password to sign in to the My Apps portal

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

Q20
HOTSPOT

You configure Microsoft Azure Active Directory (Azure AD) Connect as shown in the following exhibit.



Synchronized Directories

DIRECTORY	ACCOUNT
Adatum.com	Adatum.com\MSOL_9c71dba7d1b9

Synchronization Settings

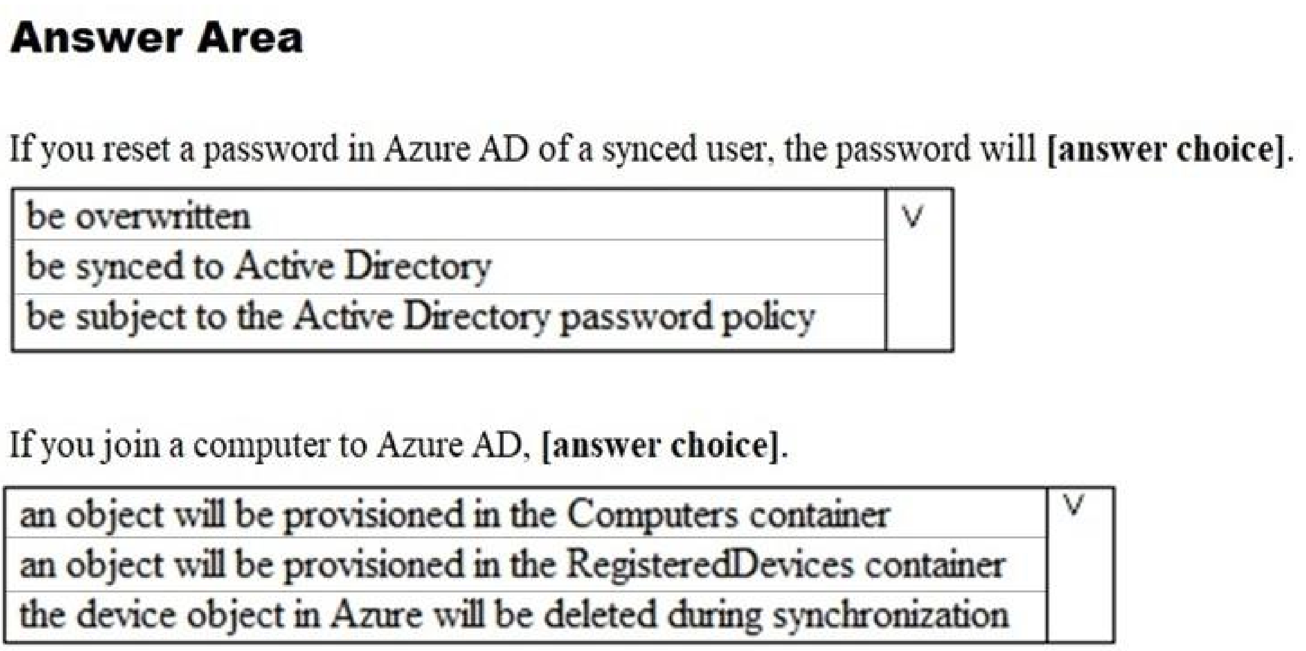
SOURCE ANCHOR
mS-DS-ConsistencyGuid
SYNC CRITERIA
AlwaysProvision
AZURE AD APP AND ATTRIBUTE FILTERING
Disabled
DIRECTORY EXTENSION ATTRIBUTE SYNC
Disabled
GROUP WRITEBACK
Disabled
PASSWORD WRITEBACK
Disabled
AUTO UPGRADE
Suspended
SQL SERVER NAME
(localdb)

USER PRINCIPAL NAME
userPrincipalName
FILTER OBJECTS TO SYNCHRONIZE BY GROUP
Disabled
DEVICE WRITEBACK
Enabled
EXCHANGE HYBRID DEPLOYMENT
Disabled
PASSWORD HASH SYNCHRONIZATION
Enabled
USER WRITEBACK
Disabled
EXCHANGE MAIL PUBLIC FOLDERS
Disabled
SQL SERVICE INSTANCE NAME
.\ADSync

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

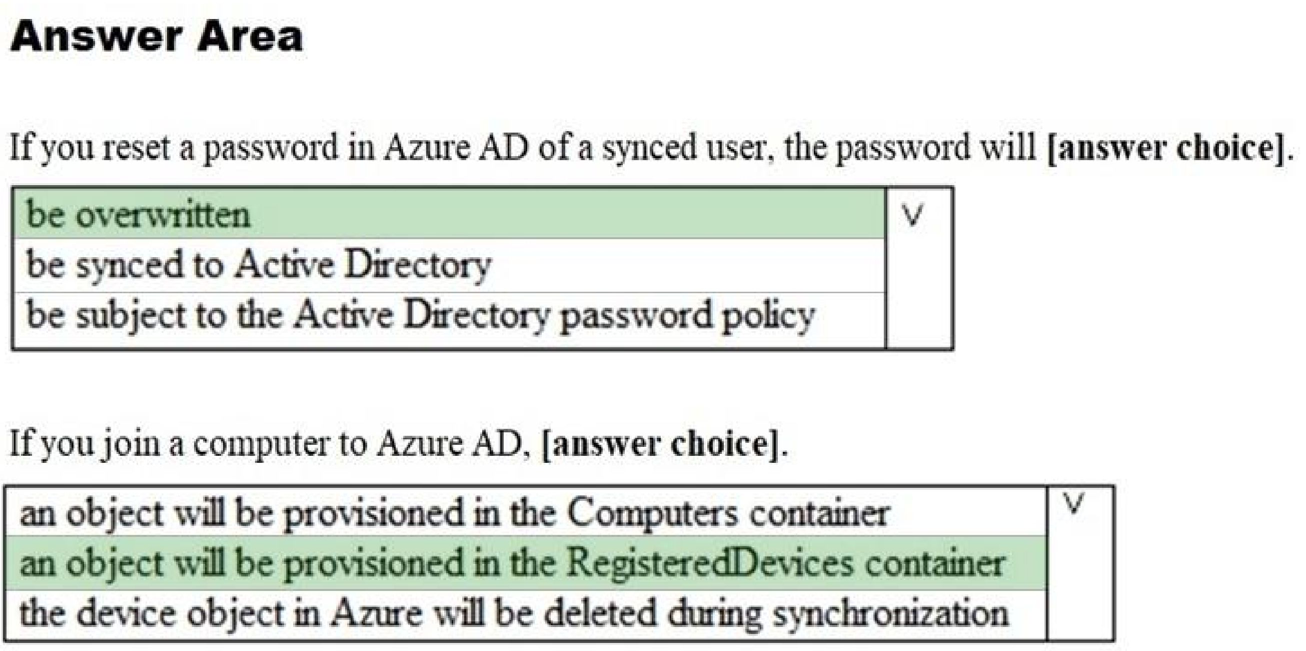
If you reset a password in Azure AD of a synced user, the password will **[answer choice]**.

- be overwritten
- be synced to Active Directory
- be subject to the Active Directory password policy

If you join a computer to Azure AD, **[answer choice]**.

- an object will be provisioned in the Computers container
- an object will be provisioned in the RegisteredDevices container
- the device object in Azure will be deleted during synchronization

Answer:



Answer Area

If you reset a password in Azure AD of a synced user, the password will **[answer choice]**.

- [✓ be overwritten]
- be synced to Active Directory
- be subject to the Active Directory password policy

If you join a computer to Azure AD, **[answer choice]**.

- an object will be provisioned in the Computers container
- [✓ an object will be provisioned in the RegisteredDevices container]
- the device object in Azure will be deleted during synchronization

Reference:

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

Q21
You have a hybrid Microsoft 365 environment. All computers run Windows 10 and are managed by using Microsoft Intune.

You need to create a Microsoft Azure Active Directory (Azure AD) conditional access policy that will allow only Windows 10 computers marked as compliant to establish a VPN connection to the on-premises network.

What should you do first?

A. From the Azure Active Directory admin center, create a new certificate
B. Enable Application Proxy in Azure AD
C. From Active Directory Administrative Center, create a Dynamic Access Control policy
D. From the Azure Active Directory admin center, configure authentication methods

Answer: A

Reference:
https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/ad-ca-vpn-connectivity- windows10

Q22
You have a Microsoft 365 subscription.

From the Microsoft 365 admin center, you create a new user.

You plan to assign the Reports reader role to the user.

You need to view the permissions of the Reports reader role.

Which admin center should you use?

A. Azure Active Directory
B. Cloud App Security
C. Security & Compliance
D. Microsoft 365

Answer: A