Pass4IT

VENDOR NAME

EXAM NAME

QUESTIONS AND ANSWERS

FREE VERSION

(LIMITED CONTENT)

Microsoft

Dumps Questions MS-500

Total Q&A: 114

Exam Name: Microsoft 365 Security Administration

Guaranteed success with Our Dumps Questions

Certification Provider: Microsoft

Exam: Microsoft 365 Security Administration

Duration: 2 Hours

Number of questions in the database: 114

Question #1

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

Correct Answer: B

Question #2

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

have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription 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

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

Question #3

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

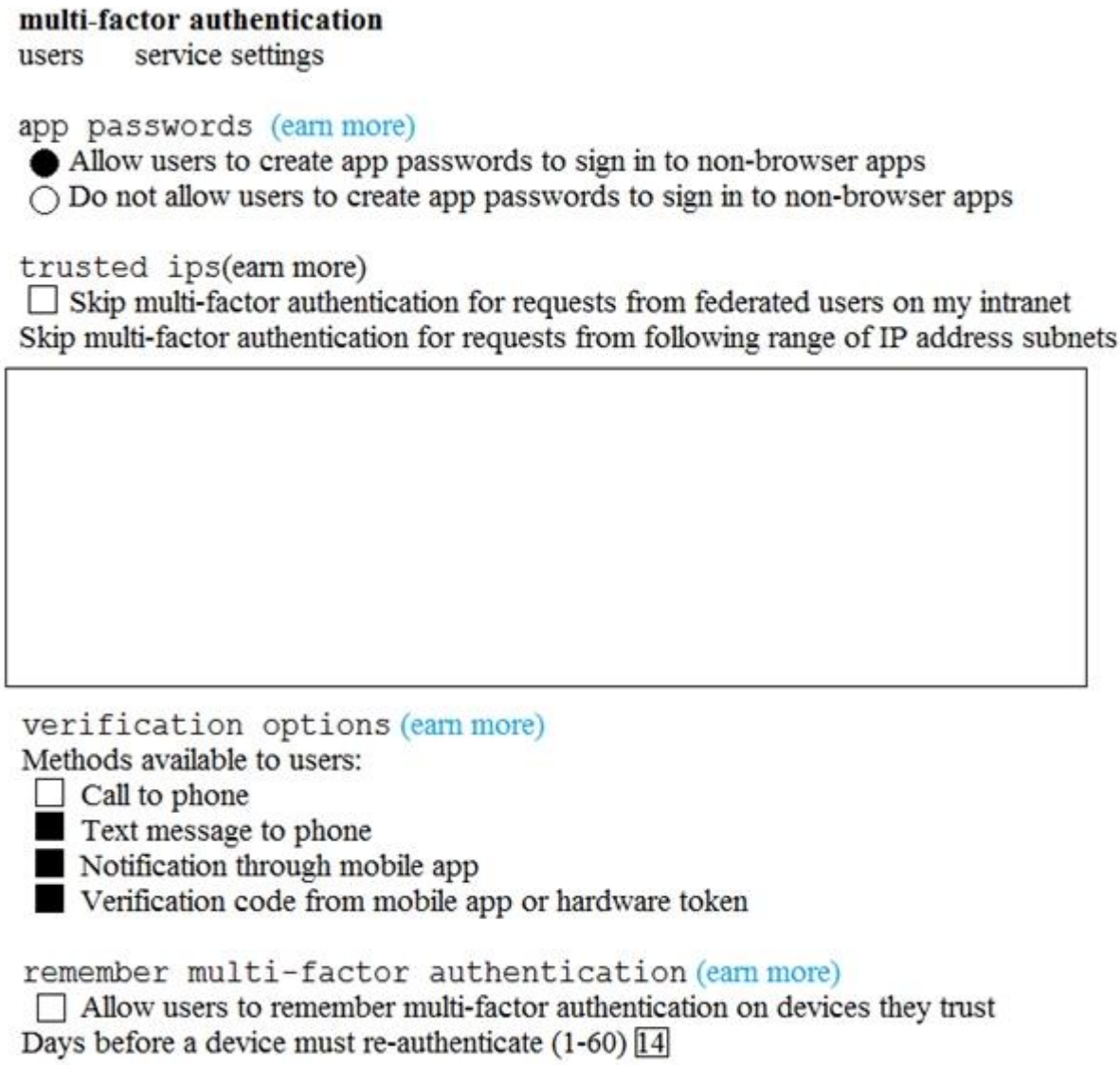
A. Yes

B. No

Correct Answer: B

Question #4

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.)



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	V
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	V
Must use app passwords for legacy apps	
Must use an app password to sign in to the My Apps portal	

Correct
Answer:

Answer Area

User1:

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

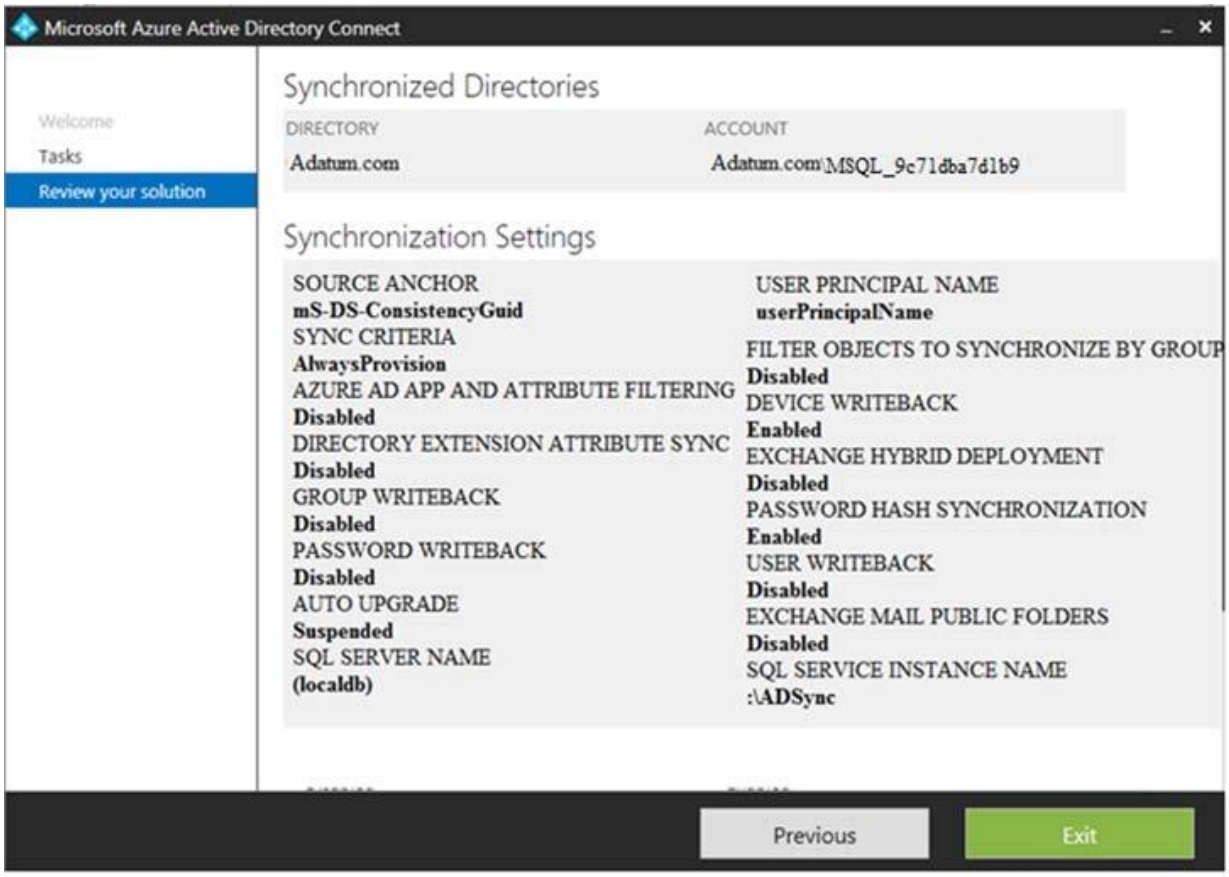
User2:

Can sign in to the My Apps portal without using MFA	V
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

Question #5

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



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, the password will **[answer choice]**.

be overwritten	V
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	V
an object will be provisioned in the RegisteredDevices container	
the device object in Azure will be deleted during synchronization	

Correct
Answer:

Answer Area

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

be overwritten	V
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	V
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