

Demo Questions

Microsoft MS-500 Exam

Microsoft 365 Security Administration

Thank you for downloading MS-500 Exam PDF

Question #1 Topic 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 #2Topic 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 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 #3Topic 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 Source Anchor settings.

Does that meet the goal?

- A. Yes
- B. No

Correct Answer: B

Question #4Topic 1

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 ([earn 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([earn 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

verification options ([earn 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 ([earn more](#))

Allow users to remember multi-factor authentication on devices they trust
Days before a device must re-authenticate (1-60)

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

Display name	Username	MFA status
User1	<u>User1@contoso.com</u>	Enabled
User2	<u>User2@contoso.com</u>	Enabled
User3	<u>User3@contoso.com</u>	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 #5Topic 1

HOTSPOT -

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

The screenshot shows the Microsoft Azure Active Directory Connect console. On the left, there is a navigation pane with 'Welcome', 'Tasks', and 'Review your solution' (highlighted in blue). The main area is titled 'Synchronized Directories' and shows a table with two columns: 'DIRECTORY' and 'ACCOUNT'. The 'DIRECTORY' column contains 'Adatum.com' and the 'ACCOUNT' column contains 'Adatum.com\MSQL_9e71dba7d1b9'. Below this is the 'Synchronization Settings' section, which is a table of settings with their current status.

DIRECTORY	ACCOUNT
Adatum.com	Adatum.com\MSQL_9e71dba7d1b9

SETTING	STATUS
SOURCE ANCHOR	mS-DS-ConsistencyGuid
USER PRINCIPAL NAME	userPrincipalName
SYNC CRITERIA	AlwaysProvision
FILTER OBJECTS TO SYNCHRONIZE BY GROUP	Disabled
AZURE AD APP AND ATTRIBUTE FILTERING	Disabled
DEVICE WRITEBACK	Enabled
DIRECTORY EXTENSION ATTRIBUTE SYNC	Disabled
EXCHANGE HYBRID DEPLOYMENT	Disabled
GROUP WRITEBACK	Disabled
PASSWORD HASH SYNCHRONIZATION	Enabled
PASSWORD WRITEBACK	Disabled
USER WRITEBACK	Disabled
AUTO UPGRADE	Suspended
EXCHANGE MAIL PUBLIC FOLDERS	Disabled
SQL SERVER NAME	(localdb)
SQL SERVICE INSTANCE NAME	:ADSync

At the bottom of the console, there are two buttons: 'Previous' (disabled) and 'Exit' (active).

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>