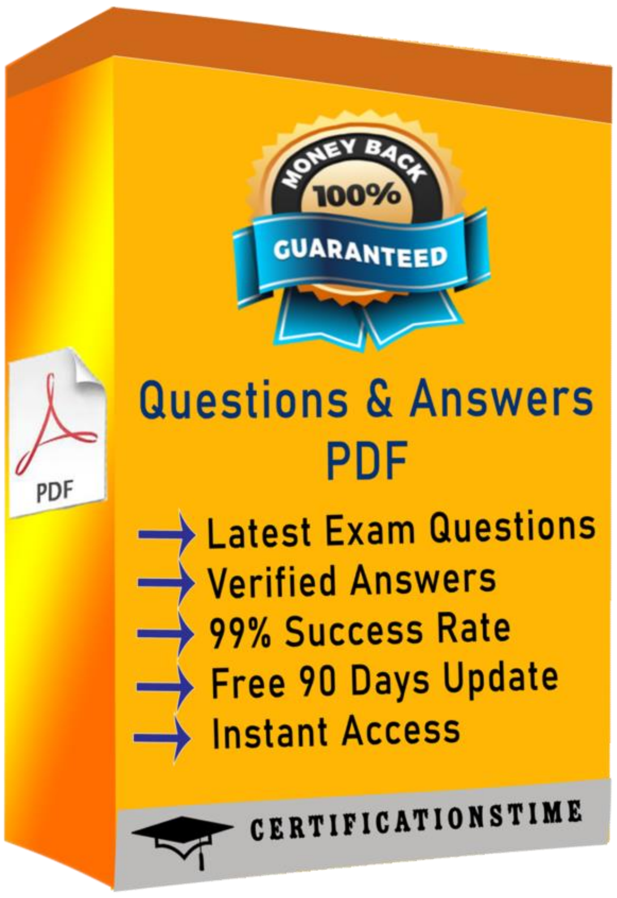
Microsoft

MS-100 Dumps

Microsoft 365 Identity and Services

https://certificationstime.com/



QUESTION 1

Your company recently purchased a Microsoft 365 subscription.
You enable Microsoft Azure Multi-Factor Authentication (Ml A) for all 500 users in the Azure Active Directory (Azure AD) tenant.
You need to generate a report that lists all the users who completed the Azure MFA registration process. What is the best approach to achieve the goal? More than one answer choice may achieve the goal. Select the BEST answer.

- A. From Azure Cloud Shell, run the Get-AzureADUser cmdlet.
- B. From Azure Cloud Shell, run the Get-MsolUser cmdlet
- C. From the Azure Active Directory admin center, use the MFA Server blade.
- D. From the Azure Active Directory admin center, use the Risky sign-ins blade.

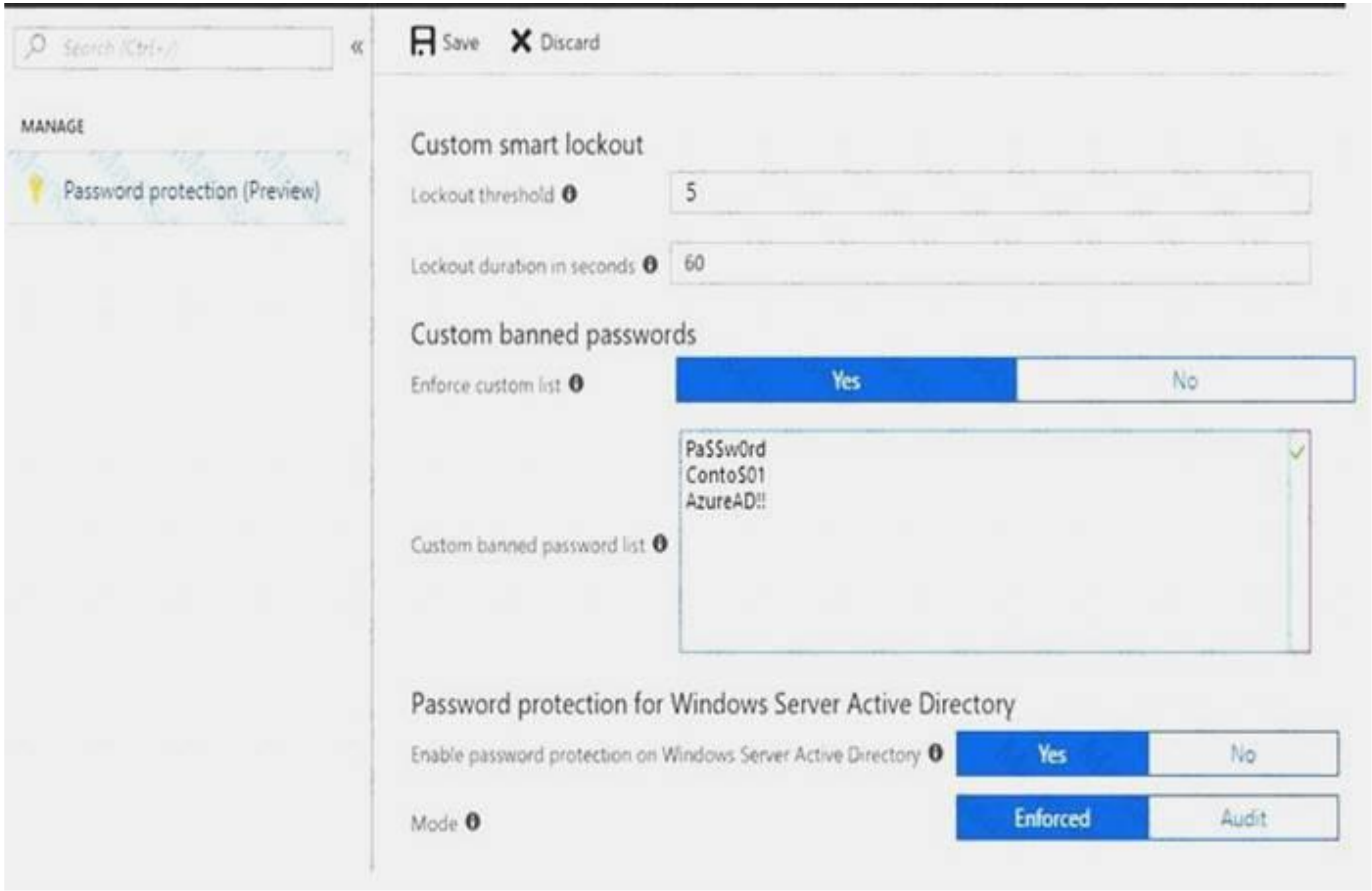
Answer: B

Explanation:

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

QUESTION 2

You have a Microsoft 365 Enterprise subscription.
You create a password policy as shown in the following exhibit.



Custom smart lockout

Lockout threshold: 5

Lockout duration in seconds: 60

Custom banned passwords

Enforce custom list: [✓ Yes] No

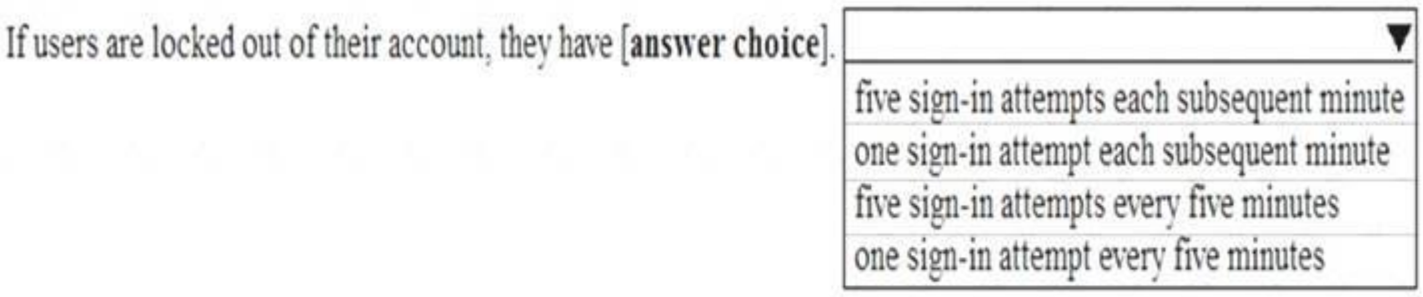
Custom banned password list:
PaSSw0rd
ContoS01
AzureAD!!

Password protection for Windows Server Active Directory

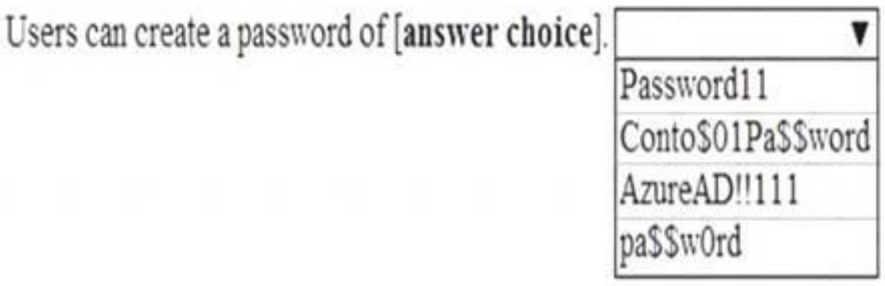
Enable password protection on Windows Server Active Directory: [✓ Yes] No

Mode: [✓ Enforced] Audit

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.



If users are locked out of their account, they have [answer choice].
- five sign-in attempts each subsequent minute
- one sign-in attempt each subsequent minute
- five sign-in attempts every five minutes
- one sign-in attempt every five minutes



Users can create a password of [answer choice].
- Password11
- Conto$01Pa$$word
- AzureAD!!111
- pa$$w0rd

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad

QUESTION 3

Note: This question it part of a series of questions that present the same scenario. Cacti 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.

Your company has a Microsoft Office 36S tenant.

You suspect that several Office 365 features were recently updated.

You need to view a last of the features that were recently updated in the tenant. Solution: You use Dashboard in Security & Compliance.

Does this meet the goal?

- A. Yes
- B. NO

Answer: B

QUESTION 4

Your network contains an Active Directory domain named contoso.com. The domain contains five domain controllers.

You purchase Microsoft 365 and plan to implement several Microsoft 365 services.

You need to identify an authentication strategy for the planned Microsoft 365 deployment. The solution must meet the following requirements:

- Ensure that users can access Microsoft 365 by using their on-premises credentials.
- Use the existing server infrastructure only.
- Store all user passwords on-premises only.
- Be highly available.

Which authentication strategy should you identify?

- A. pass-through authentication and seamless SSO
- B. pass-through authentication and seamless SSO with password hash synchronization
- C. password hash synchronization and seamless SSO
- D. federation

Answer: A

QUESTION 5

You have a Microsoft 365 Enterprise subscription.

You have a conditional access policy to force multi factor .mthentication when accessing Microsoft SharePoint from a mobile device

You need to view which users authenticated by using multi factor authentication. What should you do?

- A. From the Microsoft 36S admin center, view the Security Compliance reports.
- B. From the Azure Active Directory admin center, view the user sign-ins.
- C. From the Microsoft 365 admin center, view the Usage reports.
- D. From the Azure Active Directory admin center, view the audit logs.

Answer: B

Explanation:

References:

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

Full Access

https://certificationstime.com/updated/ms-100-exam-dumps-pdf/