Question 1
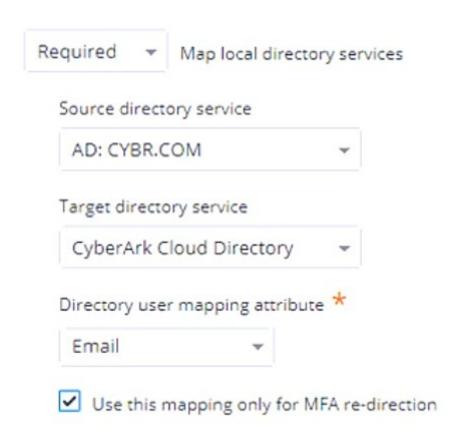
Refer to the exhibit.

If an Authentication Policy is configured as shown in the exhibit, which statement is correct?

Local Account Linking

Link user accounts between two directory services.

Required ▾ Map local directory services

Source directory service

AD: CYBR.COM ▾

Target directory service

CyberArk Cloud Directory ▾

Directory user mapping attribute *

Email ▾

☑ Use this mapping only for MFA re-direction

Options:

A- The Initial MFA challenge will be sent to the account in CyberArk Cloud Directory (Tarqet).

B- Upon successful logon, the user will be logged in as the account in CyberArJS Cloud Directory (Target).

C- Future MFA challenges will be sent to the account in AD (Source).

D- If there is no matching email between two accounts in AD (Source) and CyberArt Cloud Directory (Target), the mapping will then look for a matching User ID.

Answer:

A

Question 2

Your organization wants to implement passwordless authentication for business critical web applications. CyberArk Identity manages access to these applications.

What can you do to facilitate the enforcement of this passwordless authentication initiative? (Choose two.)

Options:

A- Configure a certificate-based authentication policy in CyberArk Identity that only allows access to CyberArk Identity or the business

critical web applications.

B- Send an email to the affected users and get them to renew their authentication token(s).

C- Roll out the CyberArk Windows Cloud Agent to the affected endpoints.

D- Refresh the endpoint operating system and define the new authentication method.

E- Roll out Secure Web Sessions to the applicable users.

Answer:

A, C

Question 3

Question Type: MultipleChoice

What is the most likely reason a CyberArk Identity admin would turn on the "Provisioning" feature within a Web App connector?

Options:

A- to ensure users are automatically on-boarded and off-boarded in a third-party application

B- to ensure users are provisioned with the appropriate devices when they start

C- to ensure the web app appears in the users' CyberArk Identity portal when they first sign in

D- to create an audit log of every time users sign into the web app

Answer:

A

Question 4

Question Type: MultipleChoice

Your Chief Executive Officer lost his phone and cannot perform MFA to log in to work.

How can you enable him to bypass MFA right away and not delay his work?

Options:

A- Add a security question to his account on his behalf.

B- Ask him to configure on-device authenticator.

C- Ask him to change his phone PIN.

D- Select the MFA Unlock action for him through the Admin Portal.

Answer:

D

Question 5

What can cause users to be prompted for unrecognized MFA factors, such as a wrong phone number or unregistered MFA factor?

Options:

A- Someone installed the CyberArk Identity mobile app on a different phone with their credentials.

B- The administrator switched authentication profiles.

C- They mistyped their username.

D- Someone registered their phone number to the wrong username.

Answer:

C

Question 6

CyberArk Identity has created a CLI integration with which vendor?

Options:

A- Amazon Web Services

B- Salesforce

C- Microsoft

D- Zoom

Answer:

A

Question 7

Which Custom Template app connectors are appropriate to use if a website does not require user authentication?

Options:

A- Bookmark

B- Browser Extension

C- SAML

D- Connect

Answer:

A

Question 8

Refer to the exhibit.

How should you configure this default authentication policy to ensure users must authenticate every time they try to access the CyberArk Identity portal or web applications?

Authentication Profile

Challenge 1	Challenge 2 (optional)

Something you have

✔ Mobile Authenticator

   Phone call

   OATH OTP Client

☑ Text message (SMS) confirmation code

   Email confirmation code

✔ QR Code

   FIDO2 Authenticator(s) (single-factor)

Something you are

✔ FIDO2 Authenticator(s) (multi-factor)

Something you know

✔ Password

   Security Question(s)

   1   Number of questions user must answer

Other

   3rd Party RADIUS Authentication

Something you have

   Mobile Authenticator

   Phone call

   OATH OTP Client

   Text message (SMS) confirmation code

   Email confirmation code

   QR Code

   FIDO2 Authenticator(s) (single-factor)

Something you are

   FIDO2 Authenticator(s) (multi-factor)

Something you know

   Password

   Security Question(s)

Other

   3rd Party RADIUS Authentication

Single Authentication Mechanism ⓘ

Options:

A- Check and enable QR Code under the 'Single Authentication Mechanism' section.

B- Check and enable Security Questions and set the number to '1'.

C- Check and Select 'Challenge Pass-Through Duration' to be 'No Pass Through'.

D- Check and Select QR Code under Challenge 1.

Answer:

C

Question 9

Question Type: MultipleChoice

You get the following error: "Not Authorized. You do not have permission to access this feature".

What is most likely the cause of the error?

Options:

A- A user tried to sign in to the wrong identity tenant.

B- A user tried to sign in before being created in Active Directory.

C- A user gave someone else access to his/her laptop.

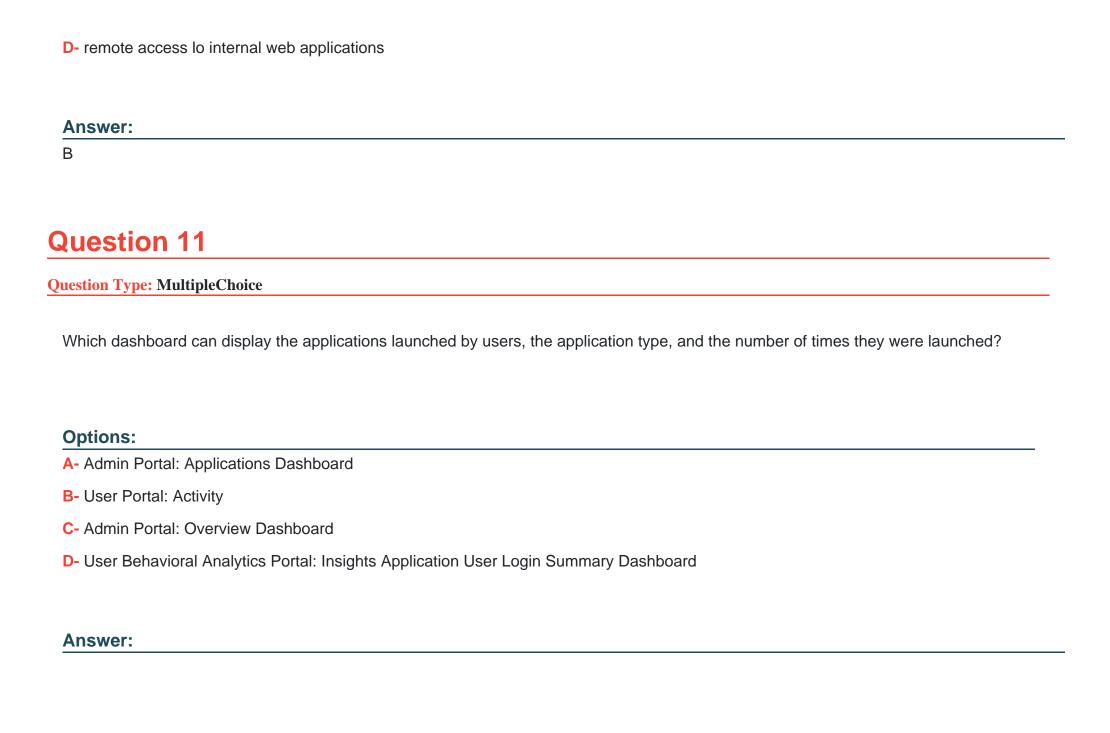**D-** A non-administrative user tried to access an administrative feature.

Answer:

D

Question 10

Question Type: **MultipleChoice**

Which feature does the CyberArk Identity Connector provide?

Options:

A- web server with SAML federation to internal web applications

B- secured, mutually authenticated, inbound communication with CyberArk Identity SaaS

C- SCIM server for connecting to CyberArk Vault

D- remote access lo internal web applications

Answer:

B

Question 11

Question Type: **MultipleChoice**

Which dashboard can display the applications launched by users, the application type, and the number of times they were launched?

Options:

A- Admin Portal: Applications Dashboard

B- User Portal: Activity

C- Admin Portal: Overview Dashboard

D- User Behavioral Analytics Portal: Insights Application User Login Summary Dashboard

Answer:

A