DUMPSBOSS.

CyberArk Defender Access (ACC-DEF)

CyberArk ACCESS-DEF

Version Demo

Total Demo Questions: 9

Total Premium Questions: 92

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1 - (SIMULATION)

Match each User Portal tab to the correct description.

ANSWER: Check the explanation for the answer

Explanation:

Match the User Portal tabs as follows:

Applications — Displays the web applications assigned to the user by the system administrator.
Devices — Lists the mobile apps/devices enrolled in CyberArk Identity.
Activity — Displays portal activity logs.
Account — Lets users change their password and modify their account information.

QUESTION NO: 2

A user's account information required for multi-factor authentication is not set up properly and is preventing the user from logging in.

What should you do?

A. Use the MFA Unlock command in the Admin Portal to suspend multifactor authentication for 10 minutes.

B. Delete the user's account and create a new one.

C. Ask the user to delete all browser cookies, then try again.

D. Change the user's director/ source from Active Directory to LDAP for authentication.

ANSWER: A

Explanation:

Use the MFA Unlock command in the Admin Portal to suspend multifactor authentication for 10 minutes. This is the appropriate recovery action when a user is unable to authenticate because the information required by their configured MFA method is incomplete, incorrect, or otherwise unavailable. An administrator can locate the affected account in the CyberArk Identity Administration portal and initiate MFA Unlock for that specific user. The command temporarily suspends the MFA requirement, giving the user a limited ten-minute opportunity to sign in and correct or re-establish the necessary authentication information. This controlled, short-duration exception maintains the account and its existing access assignments while providing a practical path to resolve the enrollment or account-information issue. After the temporary window expires, MFA protection is again required, so the user should complete the needed MFA setup during that period. CyberArk documents this administrative workflow as a way to temporarily suspend MFA for a locked-out user in its Identity Administration guidance. See the CyberArk Identity user administration documentation and the CyberArk Identity documentation portal.

QUESTION NO: 3

Refer to the exhibit.

This exhibit shows the base authentication policy for ACME Corporation. You must edit the policy to allow users to authenticate once if they fulfill certain authentication criteria.

How should you configure this policy to support BOTH?

A. Configure "Challenge Pass-Through Duration" to be "always".

B. ConfigureFID02 authenticator as Challenge 1.

C. ConfigureFID02 authenticator as Challenge 2.

D. Configure QR Code as "Single Authentication Mechanism".

ANSWER: D

Explanation:

Configure QR Code as “Single Authentication Mechanism”. In CyberArk Identity authentication policies, a single authentication mechanism provides a distinct authentication path: when a user satisfies that mechanism, the policy can accept that successful authentication without requiring the user to complete the configured challenge sequence. Selecting QR Code for this role supports an authentication-once experience for users who meet the QR-code authentication criteria, while retaining the policy’s ability to use other configured methods and challenges when the QR-code path is not applicable. QR-code authentication is designed to use the user’s registered and authenticated CyberArk Identity mobile device, providing a secure, user-friendly way to establish the user’s identity without making them enter an additional credential in the normal challenge flow. This configuration therefore directly addresses the requirement that qualifying users authenticate only once, rather than merely changing the time for which a prior challenge is remembered. CyberArk documents the policy configuration model, including authentication mechanisms and challenge controls, in its Authentication policies documentation. Additional details on supported authentication mechanisms and their configuration are available in the Authentication mechanisms documentation.

QUESTION NO: 4

An application owner wants users to request access to a SaaS application, have managers approve the requests, and ensure that accounts are created and later removed in the SaaS application as access changes.

Which two app connector features should be enabled and configured? (Select two.)

A. Workflow

B. Bookmark

C. SAML federation

D. Provisioning

E. Land and Catch

ANSWER: A D

Explanation:

Workflow provides the governed access-request and approval process. Users can request the application and configured approvers can approve or deny the request.

Provisioning manages the target application account lifecycle. When supported and configured, it can create, update, and deprovision user accounts in the third-party application as CyberArk Identity assignments and identity data change. SAML provides federation for sign-in, but it does not by itself create or remove target accounts. A Bookmark only supplies a portal link.

QUESTION NO: 5 - (SIMULATION)

A user wants to install the CyberArk Identity mobile app by using a QR code.

Arrange the steps to do this in the correct sequence.

ANSWER: Check the explanation for the answer

Explanation:

Correct sequence:

1. Log in to the CyberArk Identity **User Portal**.
2. Open the **Devices** page and select **Add Devices**.
3. Use the mobile device camera to scan the displayed **QR code**.
4. Authorize the CyberArk Identity mobile application download/install when prompted.
5. Open the application and enroll the mobile device.

The QR code is generated from the User Portal device-addition workflow. Scanning it directs the user to obtain the app, after which the device enrollment completes its association with the user account.

QUESTION NO: 6

Which browsers are supported for the "Land and Catch" feature? (Choose three.)

A. Google Chrome

B. Apple Safari

C. Microsoft Internet Explorer

D. Firefox

E. Microsoft Edge

F. Opera

ANSWER: A D E

Explanation:

Google Chrome, Firefox, and Microsoft Edge are the supported browsers for CyberArk Identity's Land and Catch capability. Land and Catch is delivered through the CyberArk Identity Browser Extension and detects a user's sign-in activity on a website. When appropriate, it enables the user to capture credentials and add the application to their CyberArk Identity User Portal, helping simplify access to applications that have not already been provisioned through the portal.

Because this workflow depends on the browser extension's supported browser integrations, the applicable browsers are the Chromium-based Google Chrome and Microsoft Edge browsers, along with Firefox. Organizations should ensure that the CyberArk Identity Browser Extension is installed, enabled, and permitted by browser or endpoint-management policy for users who need this functionality. CyberArk's Identity documentation describes browser-extension-based application access and credential capture capabilities, while the CyberArk Identity product documentation provides the current administrative guidance for configuring and using these services. See the CyberArk Identity documentation and the CyberArk Identity Security product page.

QUESTION NO: 7

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

A. Bookmark

B. Browser Extension

C. SAML

D. Connect

ANSWER: A

Explanation:

Bookmark is the appropriate Custom Template app connector for a website that does not require user authentication. A Bookmark application provides users with a tile in the CyberArk Identity User Portal that opens a specified URL directly. Since the target site is public or otherwise does not need credentials, federation, or a login workflow, the application does not

need to perform single sign-on, submit stored credentials, or invoke a browser-based authentication mechanism. This makes Bookmark suitable for publishing approved public resources, documentation portals, service-status pages, intranet pages that rely on existing network access, or other destinations where CyberArk Identity only needs to provide a convenient and centrally managed launch point. Administrators can configure the displayed application name, icon, URL, and assignment, allowing access to the link to be governed through portal visibility and policy even though the destination itself has no authentication requirement. CyberArk Identity categorizes Bookmark as an application type intended to link users to a web location rather than establish an authenticated application session. See the CyberArk Identity documentation at Applications in CyberArk Identity and the Bookmark application configuration documentation.

QUESTION NO: 8

An administrator needs to run a provisioning synchronization job immediately after correcting attribute mappings for a SaaS application.

Which administrative right is required to perform this task?

A. User Management

B. Register and Administer Connectors

C. System Enrollment

D. Application Management

ANSWER: D

Explanation:

Application Management is required because provisioning synchronization is managed from the application configuration and provisioning controls in CyberArk Identity. An administrator with this right can manage the application and manually initiate its synchronization job.

User Management controls user administration, while connector administration and endpoint enrollment rights do not grant authority to manage an application’s provisioning synchronization.

QUESTION NO: 9

Which protocols can CyberArk provide MFA for VPN? (Choose two.)

A. SAML

B. RADIUS

C. IMAP

D. TACACS

E. LDAP

ANSWER: A B

Explanation:

CyberArk provides multi-factor authentication for VPN access through **SAML** and **RADIUS** integrations. SAML is used where a VPN supports federated web-based authentication, enabling the VPN portal or gateway to redirect users to CyberArk Identity for authentication and MFA before granting access. This approach can also support single sign-on while applying CyberArk’s adaptive authentication and MFA policies. RADIUS is used for VPN appliances and clients that delegate authentication to a RADIUS server. CyberArk Identity can act as the RADIUS authentication service, validate the user’s credentials, apply the configured MFA challenge, and return the authentication result to the VPN. These two standards enable CyberArk MFA to protect remote network access across a broad range of compatible VPN products. CyberArk documents VPN and VDI protection as a use case for both RADIUS-based and SAML-based integrations, allowing

organizations to enforce stronger authentication for remote users without requiring the VPN itself to implement MFA natively. See CyberArk's secure remote access overview and the CyberArk Identity RADIUS documentation.