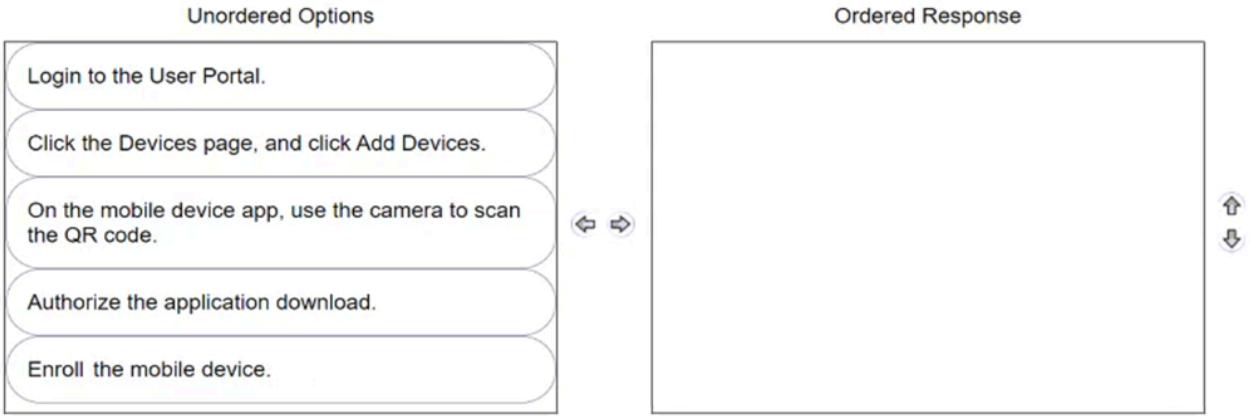
Question #1 *Topic 1*

DRAG DROP -

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.



Suggested Answer:

1. Authorize the application download
2. Enroll the mobile device:
3. Login to the User Portal:
4. Click the Devices page, and click Add Devices:
5. On the mobile device app, use the camera to scan the QR code

wuliao 1 month, 2 weeks ago

the question are outdated

upvoted 1 times

oswaldek 5 months, 3 weeks ago

1. Login to the User Portal
2. Click the Devices page, and click Add Devices
3. On the mobile device app,use the camera to scan the QR code
4. Authorize the application download
5. Enroll the mobile devices

upvoted 4 times

Question #2 *Topic 1*

Where can MFA filters be used? (Choose three.)

A. User and Admin Portal login

B. App level 2FA/MFA

C. RADIUS

D. Self-service password reset

E. Editing personal profile attributes

F. OAUTH2 connections

Suggested Answer: *ABD*

Community vote distribution

ABD (100%)

MERLIN76 4 days, 1 hour ago

Selected Answer: ABD

A,B,D - agree

upvoted 1 times

oswaldek 5 months, 3 weeks ago

Selected Answer: ABD

A,B,D - agree

upvoted 2 times

Question #3 *Topic 1*

Which 2FA/MFA options can be used if users cannot use their mobile device? (Choose two.)

A. FIDO2

B. Security questions

C. OAUTH2

D. QR code

E. Push notification app

Suggested Answer: *AB*

Community vote distribution

AB (100%)

oswaldek 5 months, 3 weeks ago

Selected Answer: AB

A,B - correct

upvoted 2 times

Question #4 *Topic 1*

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 directory source from Active Directory to LDAP for authentication.

Suggested Answer: *A*

Community vote distribution

A (100%)

oswaldek 5 months, 3 weeks ago

Selected Answer: A

A - Correct

upvoted 3 times

Question #5 *Topic 1*

Which statement is correct about the CyberArk Identity Windows Device Trust enrollment process?

A. An enrollment code is optional.

B. The endpoint does not need to be a domain-joined machine.

C. You can define the maximum number of joinable endpoints.

D. You can define the minimum number of joinable endpoints.

Suggested Answer: *C*

Community vote distribution

C (100%)

dru0pa 3 months, 2 weeks ago

Selected Answer: C

https://docs.cyberark.com/identity/latest/en/Content/Endpoints/Windows-Device-Trust.htm?Highlight=Windows%20Device%20Trust%20

upvoted 1 times

Anush2024 4 months ago

Selected Answer: C

C - correct

upvoted 1 times

oswaldek 5 months, 3 weeks ago

Selected Answer: C

C - correct

https://docs.cyberark.com/Identity/Latest/en/Content/Endpoints/Windows-Device-Trust.htm?Highlight=CyberArk%20Identity%20Windows%20Device%20Trust#EnrollWindowsmachineswithWindowsDeviceTrust

upvoted 1 times

Question #6 *Topic 1*

ACME Corporation employees access critical business web applications through CyberArk Identity. You notice a constant high volume of unauthorized traffic from 103.1.200.0/24 trying to gain access to the CyberArk Identity portal. Access to the CyberArk Identity portal is time sensitive. ACME decides to enforce IP restrictions to reduce vulnerability.
Which configuration can help achieve this?

A. Log in to the CyberArk Identity Admin portal and define the IP range of 103.1.200.0/24 into the ACME Corporation IP range.

B. Log in to the CyberArk Identity Admin portal and define the IP range of 103.1.200.0/24 into the blocked IP range.

C. Implement device trust through the Windows Cloud Agent.

D. Implement zero trust through the App Gateway.

Suggested Answer: *B*

Community vote distribution

B (100%)

oswaldek 5 months, 3 weeks ago

Selected Answer: B

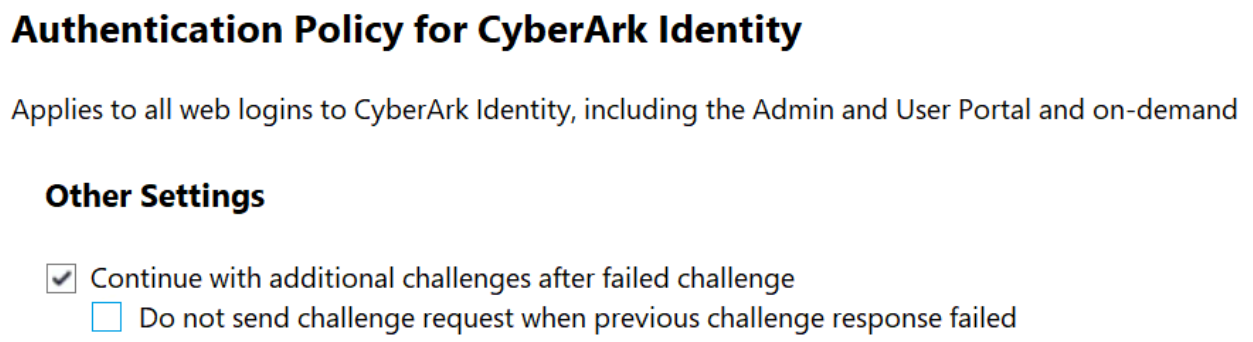
B - correct

upvoted 2 times

Question #7 *Topic 1*

Refer to the exhibit.

Which statements are correct regarding this Authentication Policy? (Choose two.)



A. Users will still be asked for their MFA even if they mistyped their username.

B. If users have set up CyberArk Mobile Authenticator as an MFA, they will still receive the Push Notification to confirm the request even if they mistyped their password.

C. Users will not be notified which challenge they failed if their login attempt failed.

D. If users have set up a Security Question as an MFA, the Security Question will not be displayed to the user to answer even if they mistyped their password.

E. If the first factor is password and the user is an Active Directory user and the Active Directory is unavailable, this setting does not matter because the user will not be able to authenticate through Active Directory credentials and will see the message "Active Directory not available".

Suggested Answer: *BC*

Community vote distribution

BC (100%)

oswaldek 5 months, 3 weeks ago

Selected Answer: BC

B,C - correct

https://docs.cyberark.com/Identity/Latest/en/Content/CoreServices/Authenticate/MFAFirstFail.htm?Highlight=%22Continue%20with%20additional%20challenges%20after%20failed%20challenge%22

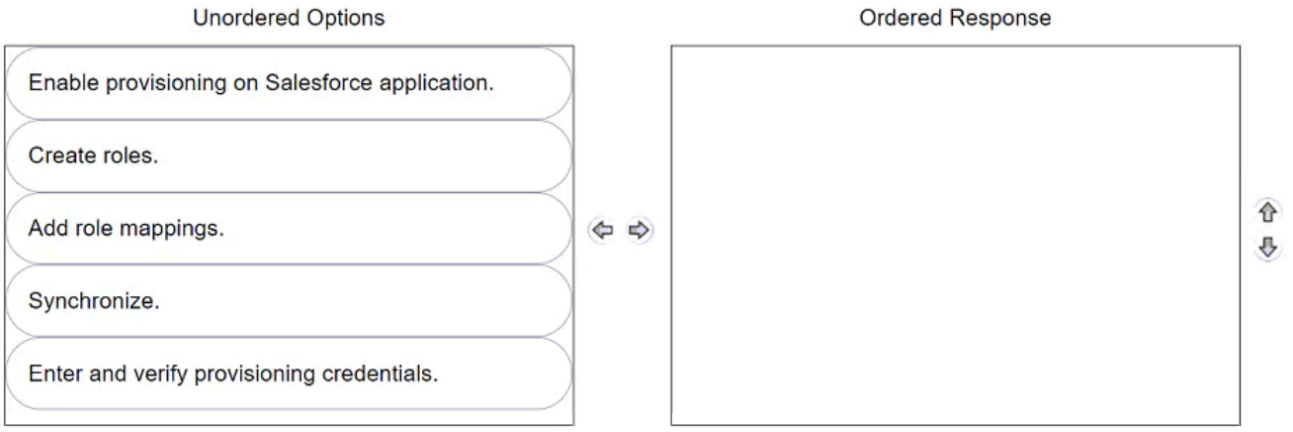
upvoted 2 times

Question #8 *Topic 1*

DRAG DROP -

Your organization wants to automatically create user accounts with different Salesforce licenses (e.g., Salesforce, Identity, Chatter External).

In CyberArk Identity, arrange the steps to achieve this in the correct sequence.



Suggested Answer:

1	**Enter and verify provisioning credentials.**
2	**Enable provisioning on Salesforce application.**
3	**Create roles.**
4	**Add role mappings.**
5	**Synchronize.**

oswaldek 5 months, 1 week ago

https://docs.cyberark.com/identity/latest/en/Content/Applications/AppsOvw/AppSpecificProv.htm?Highlight=application%20provisioning

upvoted 1 times

oswaldek 5 months, 3 weeks ago

1. Create Roles
2. Enable provisioning on Salesforce application
3. Enter and verify provisioning credentials
4. Add role mappings

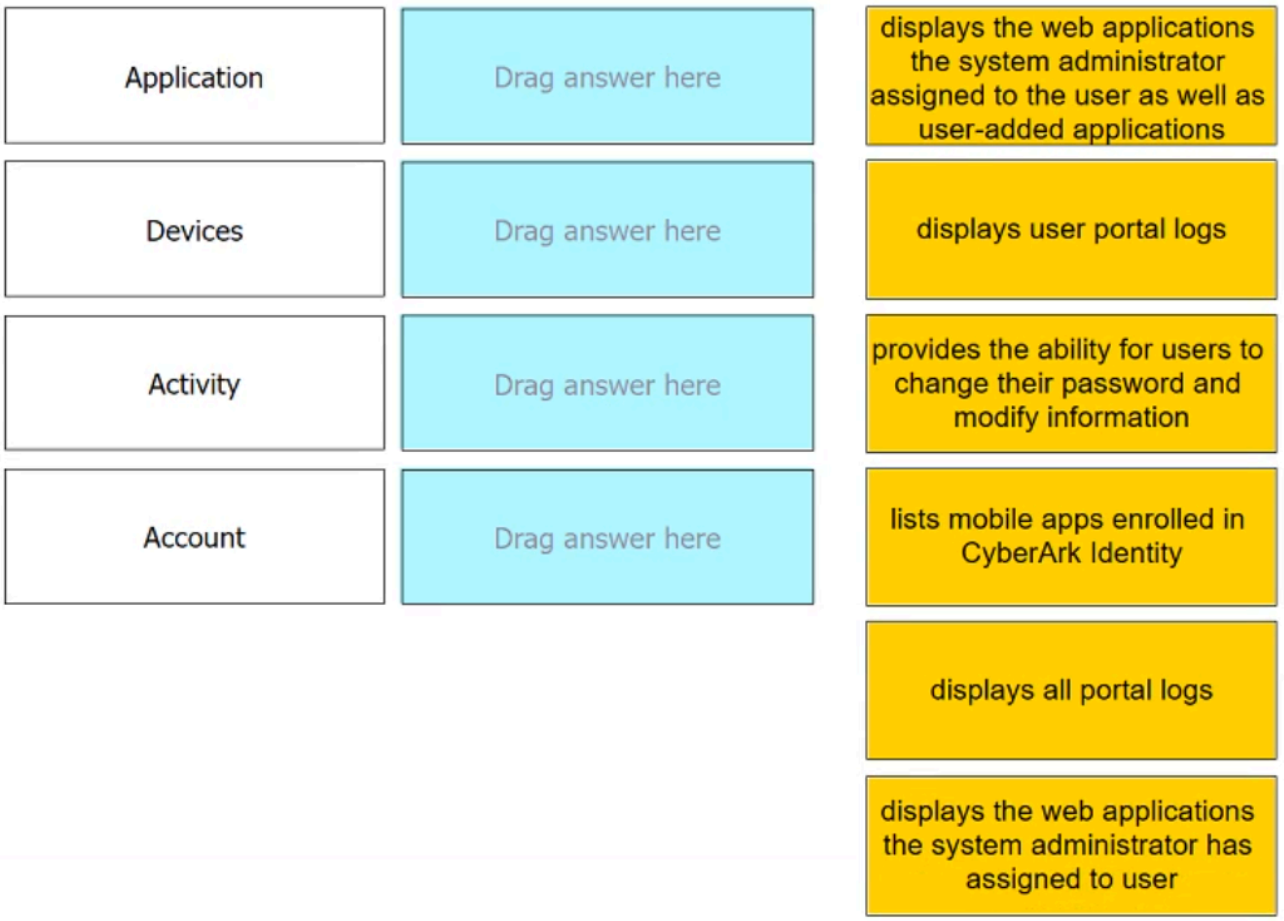
5 Synchronize

upvoted 3 times

Question #9 *Topic 1*

DRAG DROP -

Match each User Portal tab to the correct description.



Suggested Answer:

Application	displays the web applications the system administrator has assigned to the user as well as user-added applications
Devices	lists mobile apps enrolled in CyberArk Identity
Activity	displays all portal logs
Account	provides the ability for users to change their password and modify information

oswaldek 5 months, 2 weeks ago

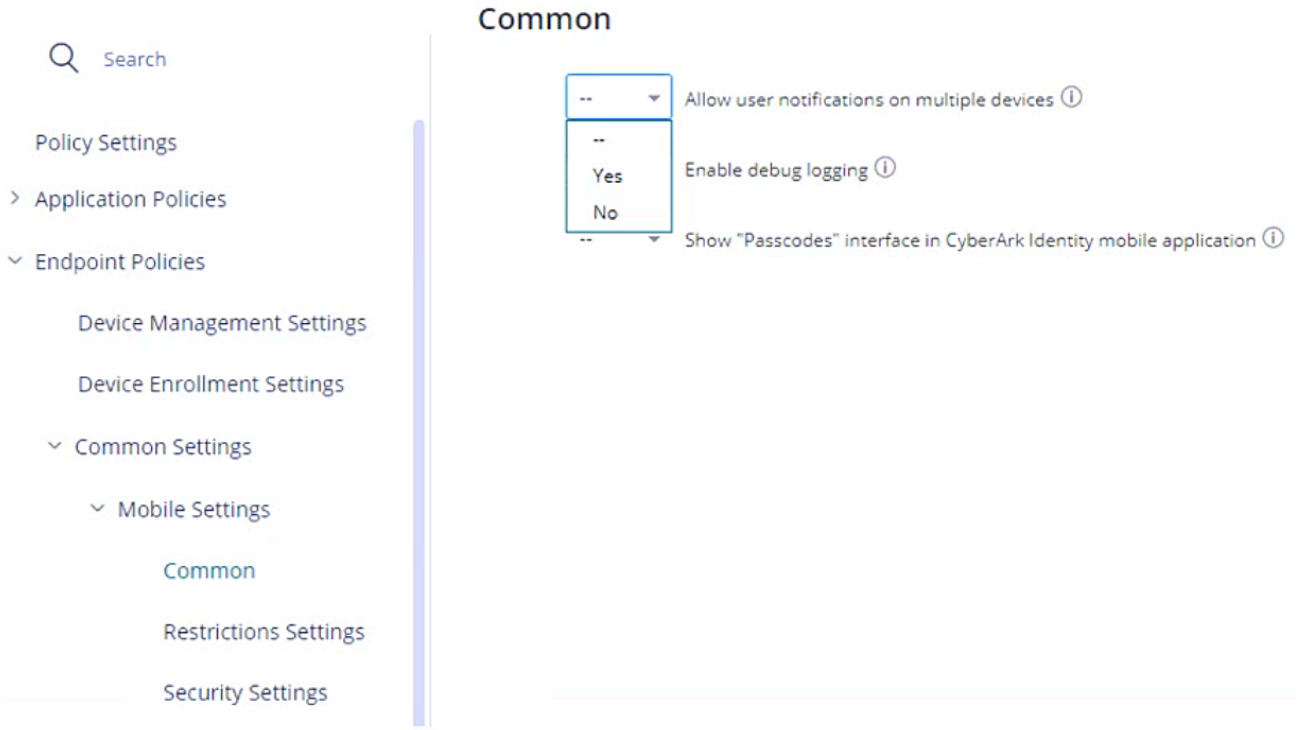
Activity - display user portal logs. The question is Tab in User Portal, not admin portal.

upvoted 3 times

Question #10 *Topic 1*

Refer to the exhibit.

Within the "Allow user notifications on multiple devices", if you leave the setting as Default (--), what happens if a user triggers a MFA Push notification and has enrolled three different devices?



A. The push notification will be sent to none of the enrolled devices.

B. The push notification will be sent to the first enrolled device only.

C. The push notification will be sent to all enrolled devices.

D. The push notification will be sent to the last enrolled device only.

Suggested Answer: *B*

Community vote distribution

B (100%)

Cark4 6 months, 1 week ago

Selected Answer: B

https://docs.cyberark.com/identity/latest/en/content/endpoints/notificationsdevices.htm?tocpath=Administrator%7CDeploy%20endpoint%20clients%7CEnroll%20mobile%20devices%7C____10

upvoted 1 times

oswaldek 11 months, 3 weeks ago

Selected Answer: B

B - correct

upvoted 2 times

Ita290188 10 months, 2 weeks ago

B - is not correct

C- correct

upvoted 1 times

Question #11 *Topic 1*

An organization previously allowed users to add their personal apps on the Identity User Portal. This will soon be disabled due to policy changes.
What is the impact to the users for personal apps previously added to the User Portal?

A. They will continue to function normally; however, users cannot add new apps.

B. They will continue to display on the Apps screen and user devices; however, they will be greyed out and unavailable for any form of interaction.

C. They will be deleted from the Apps screen and user devices.

D. They will continue to display on the Apps screen and user devices; however, an error message will display when users try to open the application.

Suggested Answer: *D*

Community vote distribution

D (100%)

Cark4 6 months, 1 week ago

Selected Answer: D

https://docs.cyberark.com/wpm/latest/en/content/applications/appsadminportal/personalappblock.htm

upvoted 1 times

oswaldek 11 months, 3 weeks ago

Selected Answer: D

D - correct

upvoted 2 times

Question #12 *Topic 1*

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

A. SAML

B. RADIUS

C. IMAP

D. TACACS

E. LDAP

Suggested Answer: *AB*

Community vote distribution

AB (100%)

oswaldek 5 months, 3 weeks ago

Selected Answer: AB

A,B - correct

upvoted 1 times

Question #13 *Topic 1*

Which device enrollment settings are valid? (Choose two.)

A. Send notification on device enrollment

B. Enable invite based enrollment

C. Minimum number of devices a user can enroll

D. Reassign the device to another user

E. Permanently delete device

Suggested Answer: *AB*

Community vote distribution

AB (100%)

chris_75 4 months, 3 weeks ago

A - Under Endpoint Policies - Device Enrolment settings

B - Under User portal - Devices - Add Device

upvoted 1 times

oswaldek 5 months, 3 weeks ago

Selected Answer: AB

A, B - correct

upvoted 3 times

Question #14 *Topic 1*

What is considered an "Identity Provider Initiated" login to an application?

A. After signing in to the CyberArk Identity portal, a user launches a SAML app by clicking an app tile.

B. After visiting a third-party web app, a user is redirected to CyberArk Identity for authentication.

C. A user visits a third party web app directly and signs in with local credentials.

D. A user signs in to the CyberArk Identity portal and takes a screenshot of the portal to send to IT.

Suggested Answer: *A*

Community vote distribution

A (100%)

oswaldek 5 months, 3 weeks ago

Selected Answer: A

A - correct

https://support.procore.com/faq/what-is-the-difference-between-sp-and-idp-initiated-sso

upvoted 1 times

Question #15 *Topic 1*

CyberArk Identity's App Gateway can be used to protect and access which option?

A. on-premises Oracle web app

B. cloud-hosted Salesforce environment

C. a corporate laptop

D. a web browser

Suggested Answer: *A*

Community vote distribution

A (100%)

oswaldek 5 months, 3 weeks ago

Selected Answer: A

A - correct

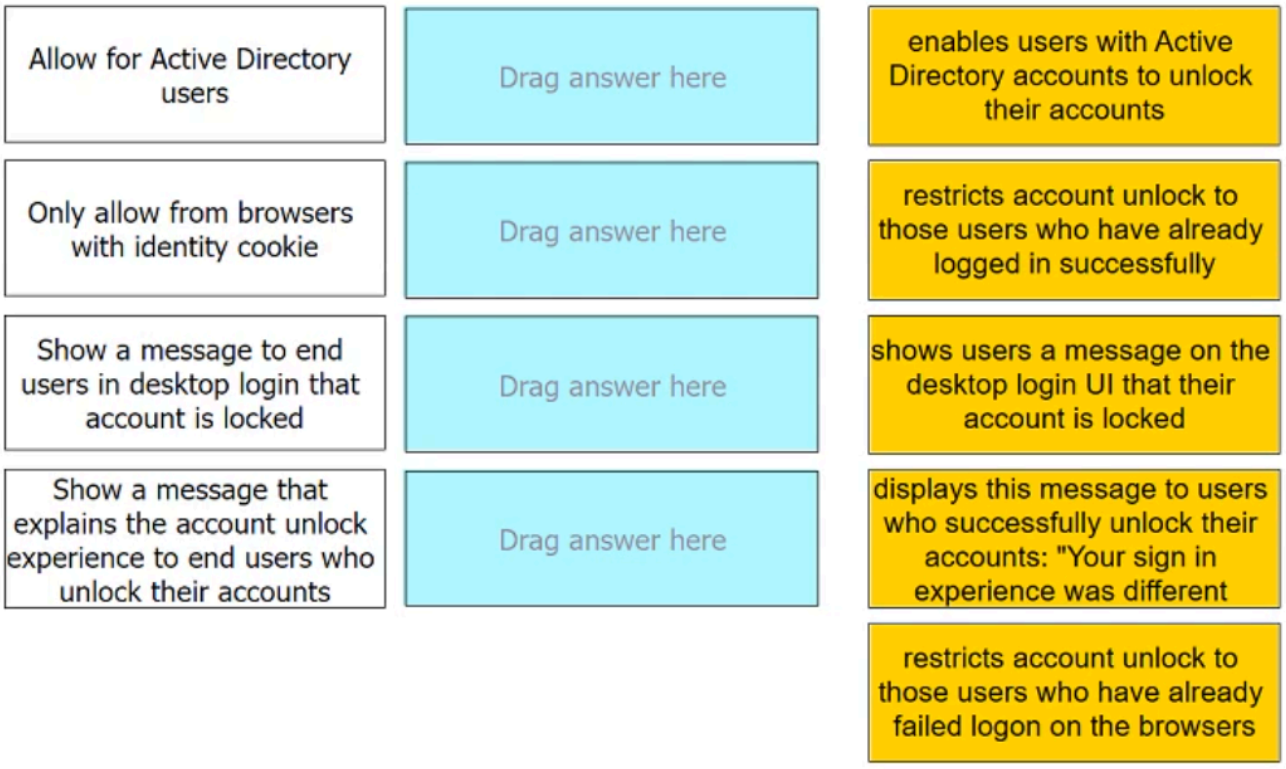
upvoted 3 times

Question #16 *Topic 1*

DRAG DROP -

Admins can enable self-service for users to unlock their accounts. There are four options under the Admin Portal Core Services > Policies > User Security Policies > Self Service > Account Unlock options.

Match each option to the correct description.



Suggested Answer:

Allow for Active Directory users	**enables users with Active Directory accounts to unlock their accounts**
Only allow from browsers with identity cookie	**restricts account unlock to those users who have already logged in successfully**
how a message to end users in desktop login that account is locked	**shows users a message on the desktop login UI that their account is locked**
Show a message that explains the account unlock experience to end users who unlock their accounts	**displays this message to users who successfully unlock their accounts: "Your sign in experience was different"**

lta290188 4 months, 1 week ago

Allow for Active Directory users = enables users with Active Directory accounts to unlock their accounts

Only allow from browsers with identity cookie = restricts account unlock to those users who have already logged in successfully

Show a message to end users in desktop login that account is locked = shows users a message on the desktop login UI that their account is locked

Show a message that explains the account unlock experience to end users who unlock their accounts = displays this message to users who successfully unlock their accounts: "Your sign in experience was different

upvoted 1 times

Question #17 *Topic 1*

Which predefined roles does CyberArk Identity provide?

A. System Administrator and Everybody

B. Manage Users and Everybody

C. System Administrator and Business Users

D. Manage Users and Business Users

Suggested Answer: *A*

Community vote distribution

A (100%)

oswaldek 5 months, 3 weeks ago

Selected Answer: A

A - correct

upvoted 3 times

Question #18 *Topic 1*

When configuring an application to use the App Gateway, you do not have to change any configurations in the application directly. You enable the application for App Gateway access in the Admin Portal and input the existing URL that users enter to open the application. You can either use an external URL that CyberArk Identity automatically generates, or you can continue using an existing internal URL.
What is a disadvantage of using an existing internal URL for App Gateway connections?

A. Existing links and bookmarks do not work outside of the corporate network.

B. Users must use different URLs depending on whether they access the application internally or externally.

C. More configuration is needed because you must upload the URL certificate and private key, and edit DNS settings.

D. Users must use the same URLs regardless of whether they access the application internally or externally and this may confuse them.

Suggested Answer: *C*

Community vote distribution

C (100%)

chris_75 4 months, 3 weeks ago

Question states: What is a disadvantage of using an existing internal URL for App Gateway connection...
https://docs.cyberark.com/identity/Latest/en/Content/Applications/AppGateway-workflow.htm

C is correct

upvoted 1 times

oswaldek 5 months, 3 weeks ago

Selected Answer: C

C - correct

upvoted 2 times

Question #19 *Topic 1*

What does the CyberArk Identity App Gateway work with? (Choose three.)

A. SAML-Compliant Apps

B. WS-Fed Enabled Apps

C. OIDC Web Apps

D. Thick Client (non-web-based Apps)

E. Terminal Services

F. Telnet

Suggested Answer: *ABC*

Community vote distribution

ABC (100%)

chris_75 4 months, 3 weeks ago

A,B,C - Correct

SAML, WS-FEd, OpenID Connect

https://docs.cyberark.com/identity/latest/en/content/Applications/AppGateway-configure-app.htm#:~:text=You%20can%20enable%20App%20gateway%20access%20for%20any,a%20few%20other%20applications%20in%20the%20application%20c

upvoted 1 times

oswaldek 5 months, 3 weeks ago

Selected Answer: ABC

A,B,C - correct

upvoted 1 times

Question #20 *Topic 1*

Which 2FA/MFA options can fulfill the "Something you are" requirement? (Choose two.)

A. email

B. CyberArk Identity mobile app

C. FIDO2

D. phone call

E. security questions

Suggested Answer: *BC*

Community vote distribution

BC (100%)

oswaldek 5 months, 3 weeks ago

Selected Answer: BC

B,C - correct

C correct, because CyberArk Identity mobile app (Mobie Authenticator) enable user to authenticate with either a one-time passcode (passkeys) and it's something you are.

upvoted 2 times

Question #21 *Topic 1*

Your team is deploying endpoint authentication onto the corporate endpoints within an organization. Enrollment details include when the enrollment must be completed, and the enrollment code was sent out to the users. Enrollment can be performed in the office or remotely (without the assistance of an IT support engineer). You received feedback that many users are unable to enroll into the system using the enrollment code.
What can you do to resolve this? (Choose two.)

A. Set maximum number of joinable endpoints to "unlimited".

B. Set Expiry Date to "Never".

C. Set the IP Address range to the user's' home network range.

D. Set a description within the enrollment code.

E. Reinstall Windows Device Trust.

Suggested Answer: *AD*

Community vote distribution

AD (100%)

chris_75 4 months, 3 weeks ago

A, B - Correct
Both settings are defined when you Generate the Bulk Enrolment Code.
Admin portal - Settings - Endpoints - Enrollment codes - Add

https://docs.cyberark.com/identity/Latest/en/Content/Endpoints/Windows-Device-Trust.htm?TocPath=Administrator%7CDeploy%20endpoint%20clients%7C____5#:~:text=Step%201%3A%20Generate%20an%20enrollment%20code%201%20In,Click%

upvoted 4 times

oswaldek 5 months, 3 weeks ago

Selected Answer: AD

A,D - correct
A obvious, D because the rest of the answers are wrong.

upvoted 1 times

Question #22 *Topic 1*

Which options are available with Self-Service Password Reset? (Choose three.)

A. Enable users with Active Directory accounts who have forgotten their password to log in and reset it.

B. Perform Self-Service Password Reset for the Organization's corporate accounts, such as Twitter, Facebook, or Instagram.

C. Users must log in after a password reset.

D. A maximum number of times can be specified that users can reset their password within a specific timeframe.

E. Users must respond to a CAPTCHA before resetting their password.

F. Use Helpdesk Caller Identity (Identity Verification) to confirm user identity.

Suggested Answer: *ACD*

Community vote distribution

ACD (100%)

oswaldek Highly Voted 5 months, 3 weeks ago

Selected Answer: ACD

A,C,D - correct

https://docs.cyberark.com/Identity/Latest/en/Content/CoreServices/UsersRoles/SelfServiceOptions.htm?Highlight=self-service%20password%20reset#ConfigureselfservicepasswordresetSSPR

upvoted 5 times

chris_75 Most Recent 4 months, 3 weeks ago

A, C, D

All 3 option under Self Service page.

B - wrong: Can not perform SSPR for B2C accounts

E - wrong: Can use CAPTCHA for consecutive failed logon attempts - Under Settings - Authentication - Security Settings - CAPTCHA settings

E. Users must respond to a CAPTCHA before resetting their password.

upvoted 2 times

Question #23 *Topic 1*

When can 2FA/MFA be prompted? (Choose two.)

A. when clicking on an app tile while in the User Portal

B. after clicking on the Forgot Your Password link

C. when making changes to a policy while in the Admin Portal

D. when exporting a compliance report while in the Admin Portal

E. when adding a new web app

Suggested Answer: *AB*

Community vote distribution

AB (100%)

oswaldek 5 months, 3 weeks ago

Selected Answer: AB

A, B - correct

B: https://docs.cyberark.com/Identity/Latest/en/Content/CoreServices/UsersRoles/SelfServiceOptions.htm?Highlight=forgot%20password%20mfa#ConfigureselfservicepasswordresetSSPR

upvoted 4 times

Question #24 *Topic 1*

What is the purpose of the Infinite Apps feature offered by CyberArk Identity?

A. It provides an easy way to find all the SAML-enabled apps that exist online.

B. It automatically downloads the desktop version of all your web apps.

C. It provides the ability to launch apps in any web browser.

D. If facilitates adding User-Password web apps not in the CyberArk Identity App Catalog.

Suggested Answer: *D*

Community vote distribution

D (100%)

chris_75 4 months, 3 weeks ago

D is correct

https://docs.cyberark.com/wpm/latest/en/Content/Applications/BrowserExtension/AddWebAppsInfinite.htm#:~:text=Infinite%20Apps%20is%20a%20featu

upvoted 2 times

oswaldek 5 months, 3 weeks ago

Selected Answer: D

D - correct

upvoted 3 times

Question #25 *Topic 1*

Which statement is true about the app gateway?

A. For applications that use the App Gateway, the connection from the user travels the same network pathways you already have and CyberArk Identity connects to the CyberArk Identity Connector through the firewall.

B. For applications that use the App Gateway, the connection from the user travels different network pathways and CyberArk Identity connects to the CyberArk Identity Connector through a separate connection from the firewall.

C. On the App Gateway page, you can configure the application to enable users to access it if they are logging in from an external location.

D. App gateway supports on-premises apps and web applications running on HTTPS only.

Suggested Answer: *A*

Community vote distribution

A (100%)

chris_75 4 months, 3 weeks ago

A - correct

https://docs.cyberark.com/identity/latest/en/content/Applications/AppGateway.htm#:~:text=For%20applications%20that%20use%20the%20App%20Gatev

upvoted 1 times

oswaldek 5 months, 3 weeks ago

Selected Answer: A

A - correct

upvoted 2 times

Question #26 *Topic 1*

When a user enrolls a mobile device (iOS or Android) without enabling mobile device management, what happens? (Choose three.)

A. The device is added to the Endpoints page in the Admin and User portals.

B. The web applications assigned to the user are added to the Web Apps screen in the CyberArk Identity mobile app.

C. The associated mobile applications are added and available for deployment automatically.

D. The mobile device policies defined in the CyberArk Cloud Directory policy service policy set are installed.

E. The device's model name, serial number, OS number, and Network Carrier information will be uploaded to the Identity portal.

F. The mobile phone can now be used as a MFA Authentication Factor.

Suggested Answer: *BEF*

Community vote distribution

BEF (100%)

chris_75 4 months, 3 weeks ago

A - wrong as it is added to Admin portal only

B,E,F

upvoted 2 times

Darkspore 5 months, 1 week ago

A is wrong because Endpoints only appears in Admin portal. In User portal it is Devices.

upvoted 3 times

oswaldek 5 months, 3 weeks ago

Selected Answer: BEF

B, E, F

E proably correct - not all information are available from user portal perspective, but most of them is visible.

A proably not correct - I have enrolled mobile devices single sign-on and i don't see them in Endpoints page in the admin portal. In user portal mobile devices is visible under "Devices"

upvoted 4 times

Question #27 *Topic 1*

As part of compliance regulation, ACME Corporation is enforcing MFA for its critical business web-based application. To increase security and MFA compliance, CyberArk recommends selecting mechanisms from different categories. Within the authentication policy, ACME Corporation made the requirement to configure an authentication mechanism with "Something you know".
Which authentication mechanism meets this requirement?

A. Phone Call

B. Security Question

C. Text Message (SMS) Confirmation Code

D. FIDO2 Authenticators

Suggested Answer: *B*

Community vote distribution

B (100%)

oswaldek 5 months, 3 weeks ago

Selected Answer: B

B - correct

upvoted 1 times

Question #28 *Topic 1*

Your organization wants to limit access to the CyberArk Identity user portal to only corporate issued domain-joined laptops without the use of a VPN.
How can you achieve this?

A. Use the Windows Device Trust agent with certificate-based authentication.

B. Use the Windows Cloud Agent and CyberArk Identity Connector with Integrated Windows Authentication (IWA).

C. Define a range of internal corporate IP addresses and use them to restrict access.

D. Use the CyberArk Conjur integration.

Suggested Answer: *A*

Community vote distribution

A (100%)

oswaldek 5 months, 3 weeks ago

Selected Answer: A

A - correct

upvoted 1 times

Question #29 *Topic 1*

What does enabling "Workflow" allow within an app connector?

A. ability to enable approval workflows for a user request to access the app

B. ability for workflows to link one app with another app

C. ability for a workflow to create, update, and delete users within a 3rd party app

D. workflows that automatically notify admins when a user logs in to the app

Suggested Answer: *A*

Community vote distribution

A (100%)

oswaldek 5 months, 3 weeks ago

Selected Answer: A

A - correct

upvoted 1 times

Question #30 *Topic 1*

Which settings can help minimize the number of 2FA / MFA prompts? (Choose two.)

A. Challenge Pass-Through Duration

B. RADIUS Connections

C. OATH OTP

D. IP Address filter

E. Port mapping

Suggested Answer: *AD*

Community vote distribution

AD (100%)

oswaldek 5 months, 3 weeks ago

Selected Answer: AD

A, D - correct

upvoted 1 times

Question #31 *Topic 1*

Which risk factors contribute to the user behavior risk score? (Choose two.)

A. operating system

B. geolocation

C. device certificate

D. session cookie

E. AD joined status of device

Suggested Answer: *BE*

Community vote distribution

AB (100%)

oswaldek 5 months ago

Selected Answer: AB

Risk facktor which you can configure: Time of Day, Day of Week, Location, Device Fingerprint, Other Factors

Correct: A (Device fingerprint?), B

upvoted 1 times

Question #32 *Topic 1*

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

Suggested Answer: *ADE*

Community vote distribution

ADE (100%)

oswaldek 5 months, 3 weeks ago

Selected Answer: ADE

A, D, E - correct

upvoted 1 times