Latest Version: 6.0

Question: 1

A company has reports of users sharing sensitive Google Drive content outside their domain through third-party add-ons. You need to control which third-party apps are allowed to access users' G Suite data.
Which security feature should you use to achieve this?
Response:

A. OAuth Whitelisting
B. Configure DLP policies to prevent sharing of sensitive content with external parties.
C. Block specific API scopes for each user.
D. In the Drive SDK section, clear 'Allow users to access Google Drive with the Drive SDK API.'

Answer: A

Question: 2

The organization is concerned with third-party applications accessing contact information. As a G Suite Super Admin, you are tasked to restrict third-party access without limiting users' ability to share contacts manually.
What should you do?
Response:

A. Disable Contact Sharing.
B. Disable API access to Google Contacts and enable Directory Sharing.
C. Enable API access to Google Contacts and disable Directory Sharing.
D. Enable Contact Sharing.

Answer: B

Question: 3

Your compliance officers want to implement a new retention policy. Email will be retained for only 180 days for most users except for VIPs, who need to retain some messages indefinitely. Your VIPs' mail is already in a separate sub-organizational unit called VIPs.
Which two configurations would meet your retention needs?
(Choose two.)
Response:

A. Create a custom retention rule for the root OU of 180 days.
B. Create a custom retention rule for the VIP OU of indefinite.
C. Create a default retention rule of 180 days.
D. Create a custom retention rule for the VIP OU to indefinitely retain messages with a given label.
E. Create a default retention rule for the VIP OU to indefinitely retain messages with a given label.

Answer: C,D

Question: 4

External Company is reporting that they are not receiving messages from your users. Your users are reporting that everything is sending fine and they are not receiving bounceback messages or any notifications.
You need to determine what could be causing the non-delivery and why they aren't receiving the notifications. What should you do?
Response:

A. Ask other customers on Cloud Connect Community if they are experiencing outages.
B. Using MX Toolbox, ensure that your SPF, DKIM, and DMARC records are up to date.
C. Review the affected sent messages in the email audit log.
D. Connect to the user's mailbox and review the headers using the Google Workspace Toolbox.

Answer: C

Question: 5

Your-company. com is currently migrating to Google Workspace. Some legacy applications are still using an on-premises exchange server to send emails.
You enabled the SMTP Relay service in Google to route the messages. During an investigation it was determined that these messages are not discoverable in Google Vault.
For compliance reasons, the Legal team is requiring that these messages are retained and discoverable. What should you do?
Response:

A. Add the Exchange Server's IP as an Inbound Gateway.
B. Enable comprehensive mail storage.
C. Create a Content Compliance rule to forward a copy of every message to a Google Group.
D. Enable Gmail forwarding for exchange server.

Answer: B

Question: 6

An organization is pushing for an effective way to manage how users access corporate data from mobile devices. A recent change to the organization's wireless settings is allowing WiFi access to users who have personal devices but preventing them from accessing corporate applications and data sources.
Users with company-owned devices are not experiencing the same issue. You are tasked with troubleshooting this issue. What should you do?
Response:

A. Enable Advanced Mobile Management and approve the device.
B. Disable Advanced Mobile Management and activate the device.
C. Enable Advanced Mobile Management and unblock the device.
D. Disable Advanced Mobile Management and approve the device.

Answer: A

Question: 7

Your company has purchased a new six-story building that has 20 meeting rooms of various sizes. One of the meeting rooms is an executive conference room that only one person should be able to see and book.
You have created that executive conference room in the Google Workspace > Calendar > Resources menu and need to restrict the sharing settings for that executive conference room. What two actions should you take?
Response:

A. Delete the resource and create the meeting room as a secondary calendar on the person's Calendar account.
B. Show the meeting room as busy all the time so it never shows up as an available room.
C. Access the Settings of the Resource to assign the person permission to make changes.
D. Clear the options under Access Permissions in the Settings of the Resource so no one else has access.
E. Show the person how to monitor meetings scheduled in the room and how to cancel them.

Answer: C,D

Question: 8

Your Communications and Training Department has a Google Site that provides updated critical business information to all employees. They want to learn how often the site is being visited and how it is used.
What should you do?
Response:

A. Embed a JavaScript page counter showing usage statistics.
B. Export the Apps Usage Activity Report showing Sites activity and send the daily report to the Communications and Training Department.

C. Add a Google Analytics Web Property ID to the Site.
D. Export the Drive Audit Log filtered to show Site Views.

Answer: C

Question: 9

A company needs to create a Google group for the customer service team. The members in that group should be able to assign and track received messages, mark a topic as resolved, and add/edit tags to a topic.
What group type should you use?
Response:

A. Web forum
B. Email List
C. Q&A Forum
D. Collaborative Inbox

Answer: D

Question: 10

Your company uses Google Workspace and has acquired a subsidiary that, for business reasons, will remain indefinitely on its existing third-party collaboration platform and legacy LDAP system.
This subsidiary operates autonomously with a separate, unfederated Active Directory forest. It is anticipated that interaction between the two companies will be infrequent and primarily conducted via email.
Leadership's minimum requirement is adding employees of that subsidiary to your corporate global address book (GAL). What should you do?
Response:

A. Configure GCDS on the subsidiary LDAP to provision their users with Cloud Identity licenses on the parent domain.
B. Create a script that uses the Directory API to sync the subsidiary's contact list as shared contacts.
C. Publish a CSV file containing the subsidiary's directory for your users to upload into Google Contacts.
D. Provision the subsidiary users with G Suite accounts on the parent domain for the additional benefit of allowing collaboration in Drive.

Answer: B