DUMPSARENA

# Google Cloud Certified - Professional Collaboration Engineer

## Google Professional-Collaboration-Engineer

**Version Demo**

**Total Demo Questions: 10**

**Total Premium Questions: 80**

**Buy Premium PDF**

https://dumpsarena.com

sales@dumpsarena.com

## QUESTION NO: 1

Your company frequently hires from five to ten interns for short contract engagements and makes use of the same generically named G Suite accounts (e.g., user1@your-company.com, user2@your-company.com, user3@your-company.com). The manager of this program wants all email to these accounts routed to the manager's mailbox account also.

What should you do?

**A.** Setup address forwarding in each account's GMail setting menu.

**B.** Set up recipient address mapping in GMail Advanced Settings.

**C.** Configure an Inbound Gateway route.

**D.** Give the manager delegated access to the mailboxes.

## ANSWER: C

**Explanation:**

Reference: https://support.google.com/a/answer/2685650?hl=en

## QUESTION NO: 2

The application development team has come to you requesting that a new, internal, domainowned G Suite app be allowed to access Google Drive APIs. You are currently restricting access to all APIs using approved whitelists, per security policy. You need to grant access for this app.

What should you do?

**A.** Enable all API access for Google Drive.

**B.** Enable “trust domain owned apps” setting.

**C.** Add OAuth Client ID to Google Drive Trusted List.

**D.** Whitelist the app in the G Suite Marketplace.

## ANSWER: C

## QUESTION NO: 3

In the years prior to your organization moving to G Suite, it was relatively common practice for users to create consumer Google accounts with their corporate email address (for example, to monitor Analytics, manage AdSense, and collaborate in Docs with other partners who were on G Suite.) You were able to address active employees’ use of consumer accounts

during the rollout, and you are now concerned about blocking former employees who could potentially still have access to those services even though they don't have access to their corporate email account.

What should you do?

**A.** Contact Google Enterprise Support to provide a list of all accounts on your domain(s) that access non-G Suite Google services and have them blocked.

**B.** Use the Transfer Tool for Unmanaged Accounts to send requests to the former users to transfer their account to your domain as a managed account.

**C.** Provide a list of all active employees to the managers of your company's Analytics, AdSense, etc. accounts, so they can clean up the respective access control lists.

**D.** Provision former user accounts with Cloud Identity licenses, generate a new Google password, and place them in an OU with all G Suite and Other Google Services disabled.

**ANSWER: C**

## QUESTION NO: 4

Your Security Officer ran the Security Health Check and found the alert that “Installation of mobile applications from unknown sources” was occurring. They have asked you to find a way to prevent that from happening.

Using Mobile Device Management (MDM), you need to configure a policy that will not allow mobile applications to be installed from unknown sources.

What MDM configuration is needed to meet this requirement?

**A.** In the Application Management menu, configure the whitelist of apps that Android and iOS devices are allowed to install.

**B.** In the Application Management menu, configure the whitelist of apps that Android, iOS devices, and Active Sync devices are allowed to install.

**C.** In Android Settings, ensure that “Allow non-Play Store apps from unknown sources installation” is unchecked.

**D.** In Device Management > Setup > Device Approvals menu, configure the “Requires Admin approval” option.

**ANSWER: C**

**Explanation:**

Reference: https://support.google.com/a/answer/7491893?hl=en

## QUESTION NO: 5

Security and Compliance has identified secure third-party applications that should have access to

G Suite data. You need to restrict third-party access to only approved applications

What two actions should you take? (Choose two.)

**A.** Whitelist Trusted Apps

**B.** Disable the Drive SDK

**C.** Restrict API scopes

**D.** Disable add-ons for Gmail

**E.** Whitelist G Suite Marketplace apps

**ANSWER: A C**

## QUESTION NO: 6

Your organization syncs directory data from Active Directory to G Suite via Google Cloud Directory Sync. Users and Groups are updated from Active Directory on an hourly basis. A user's last name and primary email address have to be changed. You need to update the user's data.

What two actions should you take? (Choose two.)

**A.** Add the user's old email address to their account in the G Suite Admin panel.

**B.** Change the user's primary email address in the G Suite Admin panel.

**C.** Change the user's last name in the G Suite Admin panel.

**D.** Change the user's primary email in Active Directory.

**E.** Change the user's last name in Active Directory.

**ANSWER: A C**

## QUESTION NO: 7

Your large organization, 80,000 users, has been on Google for two years. Your CTO wants to create an integrated team experience with Google Groups, Teams Drives, and Calendar. Users will use a Google Form and Apps Script to request a new "G-Team." A "G-Team' is composed of a Google Group and a Team Drive/Secondary Calendar that is shared using that Google Group.

What two design decisions are required to implement this workflow securely? (Choose two.)

**A.** The Apps Script will need to run as a G Suite admin.

**B.** You will need a Cloud SQL instance to store "G-Team' data.

**C.** The Google Form will need to be limited to internal users only.

**D.** The Apps Script will need to run on a timed interval to process new entries.

**E.** The Google Form will need to enforce Group naming conventions.

**ANSWER: C D**

## QUESTION NO: 8

Several customers have reported receiving fake collection notices from your company. The emails were received from accounts.receivable@yourcompany.com, which is the valid address used by your accounting department for such matters, but the email audit log does not show the emails in question. You need to stop these emails from being sent.

What two actions should you take? (Choose two.)

**A.** Change the password for suspected compromised account accounts.receivable@yourcompany.com.

**B.** Configure a Sender Policy Framework (SPF) record for your domain.

**C.** Configure Domain Keys Identified Mail (DKIM) to authenticate email.

**D.** Disable mail delegation for the accounts.receivable@yourcompany.com account.

**E.** Disable “Allow users to automatically forward incoming email to another address.”

**ANSWER: A C**

## QUESTION NO: 9

The CFO just informed you that one of their team members wire-transferred money to the wrong account because they received an email that appeared to be from the CFO. The CFO has provided a list of all users that may be responsible for sending wire transfers. The CFO also provided a list of banks the company sends wire transfers to. There are no external users that should be requesting wire transfers. The CFO is working with the bank to resolve the issue and needs your help to ensure that this does not happen again.

What two actions should you take? (Choose two.)

**A.** Configure objectionable content to reject messages with the words “wire transfer.”

**B.** Verify that DMARC, DKIM, and SPF records are configured correctly for your domain.

**C.** Create a rule requiring secure transport for all messages regarding wire transfers.

**D.** Add the sender of the wire transfer email to the blocked senders list.

**E.** Enable all admin settings in Gmail's safety > spoofing and authentication.

**ANSWER: B D**

## QUESTION NO: 10

Your company uses a whitelisting approach to manage third-party apps and add-ons. The Senior VP of Sales & Marketing has urgently requested access to a new Marketplace app that has not previously been vetted. The company's Information Security policy empowers you, as a G Suite admin, to grant provisional access immediately if all of the following conditions are met:

- Access to the app is restricted to specific individuals by request only.
- The app does not have the ability to read or manage emails.
- Immediate notice is given to the Infosec team, followed by the submission of a security risk analysis report within 14 days.

Which actions should you take first to ensure that you are compliant with Infosec policy?

**A.** Move the Senior VP to a sub-OU before enabling Marketplace Settings > "Allow Users to Install Any App from G Suite Marketplace."

**B.** Confirm that the Senior VP's OU has the following Gmail setting disabled before whitelisting the app: "Let users delegate access to their mailbox."

**C.** Add the Marketplace app, then review the authorized scopes in Security > Manage API client access.

**D.** Search the G Suite support forum for feedback about the app to include in the risk analysis report.

## ANSWER: A