



PROFESSIONAL-COLLABORATION- ENGINEER^{Q&As}

Professional Collaboration Engineer

**Pass Google PROFESSIONAL-COLLABORATION-
ENGINEER Exam with 100% Guarantee**

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.passapply.com/professional-collaboration-engineer.html>

100% Passing Guarantee
100% Money Back Assurance





Following Questions and Answers are all new published by Google
Official Exam Center



VCE & PDF

PassApply.com

<https://www.passapply.com/professional-collaboration-engineer.html>
2024 Latest passapply PROFESSIONAL-COLLABORATION-ENGINEER PDF
and VCE dumps Download

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





QUESTION 1

A company has thousands of Chrome devices and bandwidth restrictions. They want to distribute the Chrome device updates over a period of days to avoid traffic spikes that would impact the low bandwidth network.

Where should you enable this in the Chrome management settings?

- A. Randomly scatter auto-updates.
- B. Update over cellular.
- C. Disable Auto update.
- D. Throttle the bandwidth.

Correct Answer: A

Reference: <https://support.google.com/chrome/a/answer/3168106?hl=en>

QUESTION 2

Your cyber security team has requested that all email destined for external domains be scanned for credit card numbers, and if found, the email must be encrypted using your cloud-based third-party encryption provider. You are responsible for configuring to meet this request.

What should you do?

- A. Create a content compliance rule on outbound mail and internal-sending mail using the predefined rule for credit card numbers, and add a custom header that your third-party encryption provider can scan for and encrypt.
- B. Create a content compliance rule on outbound mail using the predefined rule for credit card numbers, and check "Encrypt message if not encrypted".
- C. Create a content compliance rule on outbound mail using the predefined rule for credit card numbers, and add a custom header that your third-party encryption provider can scan for and encrypt.
- D. Create a content compliance rule on outbound mail using the predefined rule for credit card numbers, and check "Change route" to send to your third-party encryption provider to encrypt.

Correct Answer: D

QUESTION 3

Your company's Chief Information Security Officer has made a new policy where third-party apps should not have OAuth permissions to Google Drive. You need to reconfigure current settings to adhere to this policy.

What should you do?

- A. Access Apps > Google Workspace > Drive and Docs > Sharing Settings and disable third-party apps sharing
- B. Access the Security Menu > API Permissions > choose Drive and Disable All Access.



- C. Access the Security Menu > API Permissions > choose Drive and Disable High Risk Access.
- D. Access Apps > Google Workspace > Drive and Docs > Sharing Settings and disable sharing outside of your domain

Correct Answer: D

QUESTION 4

The application development team has come to you requesting that a new, internal, domain-owned 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.

Correct Answer: C

QUESTION 5

Your organization has just appointed a new CISO. They have signed up to receive admin alerts and just received an alert for a suspicious login attempt. They are trying to determine how frequently suspicious login attempts occur within the organization. The CISO has asked you to provide details for each user account that has had a suspicious login attempt in the past year and the number of times it occurred for each account.

What action should you take to meet these requirements?

- A. Use the login audit report to export all suspicious login details for analysis.
- B. Create a custom dashboard with the security investigation tool showing suspicious logins.
- C. Use the account activity report to export all suspicious login details for analysis.
- D. Create a custom query in BigQuery showing all suspicious login details.

Correct Answer: A

[PROFESSIONAL-COLLABORATION-ENGINEER Practice Test](#)

[PROFESSIONAL-COLLABORATION-ENGINEER Exam Questions](#)

[PROFESSIONAL-COLLABORATION-ENGINEER Braindumps](#)