

GOOGLE-WORKSPACE- ADMINISTRATOR^{Q&As}

Google Cloud Certified - Professional Google Workspace Administrator

**Pass Google GOOGLE-WORKSPACE-
ADMINISTRATOR Exam with 100% Guarantee**

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

<https://www.leads4pass.com/google-workspace-administrator.html>

100% Passing Guarantee
100% Money Back Assurance

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

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



QUESTION 1

You recently started an engagement with an organization that is also using Google Workspace. The engagement will involve highly sensitive data, and the data needs to be protected from being shared with unauthorized parties both internally and externally. You need to ensure that this data is properly secured.

Which configuration should you implement?

- A. Turn on external sharing with whitelisted domains, and add the external organization to the whitelist.
- B. Provision accounts within your domain for the external users, and turn off external sharing for that Org.
- C. Configure the Drive DLP rules to prevent the sharing of PII and PHI outside of your domain.
- D. Create a Team Drive for this engagement, and limit the memberships and sharing settings.

Correct Answer: D

Explanation: <https://support.google.com/a/users/answer/9310352#1.1>

QUESTION 2

Your company's compliance officer has requested that you apply a content compliance rule that will reject all external outbound email that has any occurrence of credit card numbers and your company's account number syntax, which is AccNo. You need to configure a content compliance rule to scan email to meet these requirements.

Which combination of attributes will meet this objective?

- A. Name the rule > select Outbound and Internal Sending > select If ANY of the following match > add two expressions: one for Simple Content Match to find AccNo, and one for predefined content match to select Credit Card Numbers > choose Reject.
- B. Name the rule > select Outbound > select If ANY of the following match > add two expressions: one for Simple Content Match to find AccNo, and one for predefined content match to select Credit Card Numbers > choose Reject
- C. Name the rule > select Outbound and Internal Sending > select If ALL of the following match > add two expressions: one for Advanced Content Match to find AccNo in the Body, and one for predefined content match to select Credit Card Numbers > choose Reject.
- D. Name the rule > select Outbound > select If ALL of the following match > add two expressions: one for Advanced Content Match to find AccNo in the Body, and one for predefined content match to select Credit Card Numbers > choose Reject.

Correct Answer: D

Explanation: <https://www.shieldq.com/en-gb/Google-apps-content-compliance>

QUESTION 3

You are supporting an investigation that is being conducted by your litigation team. The current default retention policy for mail is 180 days, and there are no custom mail retention policies in place. The litigation team has identified a user

who is central to the investigation, and they want to investigate the mail data related to this user without the user's awareness.

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

- A. Move the user to their own Organization Unit, and set a custom retention policy
- B. Create a matter using Google Vault, and share the matter with the litigation team members.
- C. Create a hold on the user's mailbox in Google Vault
- D. Reset the user's password, and share the new password with the litigation team.
- E. Copy the user's data to a secondary account.

Correct Answer: BC

Explanation: <https://support.google.com/vault/answer/2473591>

QUESTION 4

Your organization has been on Google Workspace Enterprise for one year. Recently, an admin turned on public link sharing for Drive files without permission from security. Your CTO wants to get better insight into changes that are made to the Google Workspace environment. The chief security officer wants that data brought into your existing SIEM system.

What are two ways you should accomplish this? (Choose two.)

- A. Use the Data Export Tool to export admin audit data to your existing SIEM system
- B. Use Apps Script and the Reports API to export admin audit data to your existing SIEM system.
- C. Use Apps Script and the Reports API to export drive audit data to the existing SIEM system
- D. Use the BigQuery export to send admin audit data to the existing SIEM system via custom code
- E. Use the BigQuery export to send drive audit data to the existing SIEM system via custom code.

Correct Answer: BD

QUESTION 5

Your chief compliance officer is concerned about API access to organization data across different cloud vendors. He has tasked you with compiling a list of applications that have API access to Google Workspace data, the data they have access to, and the number of users who are using the applications.

How should you compile the data being requested?

- A. Review the authorized applications for each user via the Google Workspace Admin panel.
- B. Create a survey via Google forms, and collect the application data from users.
- C. Review the token audit log, and compile a list of all the applications and their scopes.

D. Review the API permissions installed apps list, and export the list.

Correct Answer: C

Explanation: <https://support.google.com/a/answer/7281227?hl=en> <https://support.google.com/a/answer/6124308?hl=en>

[Latest GOOGLE-WORKSPACE-ADMINISTRATOR Dumps](#)

[GOOGLE-WORKSPACE-ADMINISTRATOR PDF Dumps](#)

[GOOGLE-WORKSPACE-ADMINISTRATOR VCE Dumps](#)