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.pass4itsure.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

QUESTION 1

The organization has conducted and completed Security Awareness Training (SAT) for all employees. As part of a new security policy, employees who did not complete the SAT have had their accounts suspended. The CTO has requested to

be informed of any accounts that have been re-enabled to ensure no one is in violation of the new security policy.

What should you do?

A. Enable "Suspicious login" rule - Other Recipients: CTO

B. Enable "Suspended user made active" rule - Other Recipients: CTO

C. Enable "Email settings changed" rule - -Other Recipients: CTO

D. Enable "Suspended user made active" rule and select "Deliver to" Super Administrator(s)

Correct Answer: B

Explanation: CTO must be informed when creating the Suspended user made active--A suspended user is made active by an admin Alert. Ref: https://support.google.com/a/answer/3230421?hl=en#zippy=%2Cuser-activity-alerts

QUESTION 2

As a Google Workspace administrator for your organization, you are tasked with controlling which third-party apps can access Google Workspace data. Before implementing controls, as a first step in this process, you want to review all the third-party apps that have been authorized to access Workspace data. What should you do?

A. Open Admin Console > Security > API Controls > App Access Control > Manage Third Party App Access.

B. Open Admin Console > Security > API Controls > App Access Control > Manage Google Services.

C. Open Admin Console > Security > Less Secure Apps.

D. Open Admin Console > Security > API Controls > App Access Control > Settings.

Correct Answer: A

Explanation: https://support.google.com/a/answer/7281227?hl=en#zippy=%2Cstep- manage-third-party-app-access-to-google-services-add- apps:~:text=In%20the%20Admin,App%20Access.

QUESTION 3

Your company wants to provide secure access for its employees. The Chief Information Security Officer disabled peripheral access to devices, but wants to enable 2-Step verification. You need to provide secure access to the applications using Google Workspace.

What should you do?

A. Enable additional security verification via email.

B. Enable authentication via the Google Authenticator.

C. Deploy browser or device certificates via Google Workspace.

D. Configure USB Yubikeys for all users.

Correct Answer: B

Explanation: Enable authentication via the Google Authenticator is the only secure option since USB device aren\\'t usable. Google Authenticator is the most secure option after physical key.

QUESTION 4

Your marketing department needs an easy way for users to share items more appropriately. They want to easily link-share Drive files within the marketing department, without sharing them with your entire company. What should you do to fulfil this request? (Choose two.)

A. Create a shared drive that\\'s shared internally organization-wide.

B. Update Drive sharing for the marketing department to restrict to internal.

C. Create a shared drive for internal marketing use.

D. Update the link sharing default to the marketing team when creating a document.

E. In the admin panel Drive settings, create a target audience that has all of marketing as members.

Correct Answer: CE

Explanation: https://support.google.com/a/users/answer/9310249#1.2
https://support.google.com/a/answer/9935192?hl=en#:~:text=a%20target%20audience-,Create%20a%20target%20audience,as%20Google%20Drive%2C%20to% 20make%20it%20available%20in%20users%27%20sharing%20settings.,-Before%20you%20begin
https://support.google.com/a/answer/9934697?hl=en

QUESTION 5

As the newly hired Admin in charge of Google Workspace, you learn that the organization has been using Google Workspace for months and has configured several security rules for accessing Google Drive. A week after you start your role, users start to complain that they cannot access Google Drive anymore from one satellite office and that they receive an error message that "a company policy is blocking access to this app." The users have no issue with Gmail or Google Calendar. While investigating, you learn that both this office\\'s Internet Service Provider (ISP) and the global IP address when accessing the internet were changed over the weekend. What is the most logical reason for this issue?

A. An access level was defined based on the IP range and applied to Google Drive via Context-Aware Access.

B. Under Drive and Docs > Sharing Settings, the "Whitelisted domains" list needs to be updated to add the new ISP domain.

C. The Network Mask defined in Security > Settings > SSO with 3rd Party IdPs should be updated to reflect the new IP range.

D. You need to raise a ticket to Google Cloud Support to have your new IP ranges registered for Drive API access.

Correct Answer: A