

Valid Google Google-Workspace-Administrator Test Registration - Google-Workspace-Administrator Certification Dumps



P.S. Free & New Google-Workspace-Administrator dumps are available on Google Drive shared by Pass4suresVCE:
https://drive.google.com/open?id=1NHu3cz7B6fTHWBd4UNxgrw1Hf_He6Dym

Desktop Google Cloud Certified - Professional Google Workspace Administrator (Google-Workspace-Administrator) practice exam software also keeps track of the earlier attempted Google Cloud Certified - Professional Google Workspace Administrator (Google-Workspace-Administrator) practice test so you can know mistakes and overcome them at each and every step. The Desktop Google Cloud Certified - Professional Google Workspace Administrator (Google-Workspace-Administrator) practice exam software is created and updated in a timely by a team of experts in this field. If any problem arises, a support team is there to fix the issue.

Google Workspace Administrator certification is a valuable credential for IT professionals who want to enhance their career prospects in the field of cloud computing. Google Cloud Certified - Professional Google Workspace Administrator certification exam is ideal for IT professionals who are responsible for managing and administering Google Workspace for their organizations. It is also suitable for IT professionals who want to learn how to manage and administer Google Workspace services and gain a deep understanding of the platform's features and capabilities.

>> Valid Google Google-Workspace-Administrator Test Registration <<

Free PDF Google-Workspace-Administrator - Google Cloud Certified - Professional Google Workspace Administrator Accurate Valid Test Registration

You can customize the time and Google Google-Workspace-Administrator questions of our Google Cloud Certified - Professional Google Workspace Administrator (Google-Workspace-Administrator) practice exams according to your needs. Real Google Google-Workspace-Administrator exam environment which our web-based and desktop Google-Workspace-Administrator Practice Exams create is beneficial to get accustomed to the real Google-Workspace-Administrator exam pattern.

Google Cloud Certified - Professional Google Workspace Administrator Sample Questions (Q102-Q107):

NEW QUESTION # 102

The security team for your organization is concerned about phishing attacks against your end user base. What two actions should you take to configure the strongest possible preventative measure against phishing attacks?

Choose 2 answers

- A. Force encryption on all inbound and outbound emails from your Workspace domain.

- B. Configure spoofing and authentication controls to warn end users about messages that are perceived as threats.
- C. Configure spoofing and authentication controls to quarantine messages that are perceived as threats
- D. Train end users to mark messages as spam when they see something suspicious.
- E. Enforce confidential mode for all messages sent and received from your Workspace domain

Answer: B,C

Explanation:

Access Admin Console: Go to admin.google.com and sign in with your admin account.

Navigate to Gmail Settings: In the Admin console, go to Apps > Google Workspace > Gmail > Safety.

Configure Spoofing and Authentication Controls:

Set up email authentication policies such as SPF, DKIM, and DMARC to verify incoming emails.

Enable options to quarantine messages that fail authentication checks and are perceived as threats.

Configure warnings for users to alert them about potentially harmful messages.

Create Compliance Rules: Under the Gmail settings, create rules that quarantine suspicious emails and notify users when they receive messages that might be phishing attempts.

Train Users: Educate users on how to recognize phishing attempts and the importance of marking suspicious emails as spam.

By configuring these settings, you enhance the security against phishing attacks by both automatically handling suspected threats and making users aware of potential dangers.

Reference

Protect against spam and phishing with Gmail

Set up email authentication (SPF, DKIM, DMARC)

NEW QUESTION # 103

As a Workspace Administrator, you want to keep an inventory of the computers and mobile devices your company owns in order to track details such as device type and who the device is assigned to. How should you add the devices to the company-owned inventory?

- A. Download the company owned inventory template CSV file from the admin panel, enter the asset tag of the devices, and upload it back to the company owned inventory in the admin panel.
- B. Download the company owned inventory template CSV file from the admin panel, enter the Device OS, asset tag and upload it back to the company owned inventory in the admin panel.
- C. Download the company owned inventory template CSV file from the admin panel, enter the Device OS, serial number and upload it back to the company owned inventory in the admin panel.
- D. Download the company owned inventory template CSV file from the admin panel, enter the serial number of the devices, and upload it back to the company owned inventory in the admin panel.

Answer: D

Explanation:

<https://support.google.com/a/answer/7129612?hl=en#zippy=%2Cassigning-devices%2Cadd-android-devices-for-the-most-management-features~:text=Add%20devices%20to,and%20upload%20status.>

NEW QUESTION # 104

Your organization recently implemented context-aware access policies for Google Drive to allow users to access Drive only from corporate managed desktops. Unfortunately, some users can still access Drive from non-corporate managed machines. What preliminary checks should you perform to find out why the Context-Aware Access policy is not working as intended? (Choose two.)

- A. Check whether device policy application is installed on users' devices.
- B. Delete and recreate a new Context-Aware Access device policy.
- C. Confirm that the user has at least a Google Workspace Business license.
- D. Check whether Endpoint Verification is installed on users' desktops.
- E. Confirm that the user has a Google Workspace Enterprise Plus license.

Answer: D,E

Explanation:

To ensure that the Context-Aware Access policy is working correctly, perform the following checks:

- * Confirm Google Workspace License:
 - * Verify that the user has a Google Workspace Enterprise Plus license. Context-Aware Access is a feature available only to Enterprise Plus customers.
 - * In the Admin console, navigate to Billing > Subscriptions and confirm the license type assigned to the user.
 - * Check Endpoint Verification:
 - * Ensure that Endpoint Verification is installed and active on users' desktops.
 - * Go to the Admin console, navigate to Devices > Endpoint Verification.
 - * Check the list of devices to confirm that Endpoint Verification is installed and reporting the status of users' devices.
 - * Additional Steps:
 - * Ensure that policies are correctly configured and applied to the relevant Organizational Units (OUs).
 - * Verify that the Context-Aware Access policies are correctly set up in Security > Context-Aware Access.
- By confirming the correct license and ensuring Endpoint Verification is installed, you can troubleshoot and resolve issues related to Context-Aware Access policy enforcement.
- References:
- * Set up Context-Aware Access
 - * Endpoint Verification overview

NEW QUESTION # 105

A user does not follow their sign-in pattern and signs in from an unusual location. As an admin, what should you do in response to this alert for this user during this investigation?

- **A. Investigate the account for unauthorized activity in the Login and Security Audit Log**
- B. Add Two Factor Authentication to the Domain
- C. Enhance your security alerts for tracking sign-in patterns
- D. First, suspend the account and then investigate

Answer: A

NEW QUESTION # 106

Your organization is part of a highly regulated industry with a very high turnover. In order to recycle licenses for new employees and comply with data retention regulations, it has been determined that certain Google Workspace data should be stored in a separate backup environment.

How should you store data for this situation?

- A. Write a script and use Google Workspace APIs to access and download user data.
- B. Train users to use Google Takeout and store their archives locally.
- **C. Use a third-party tool to configure secure backup of Google Workspace data.**
- D. Use routing rules to dual-deliver mail to an on-premises SMTP server and Google Workspace.

Answer: C

Explanation:

Evaluate Third-Party Backup Solutions: Identify third-party tools that offer secure backup solutions for Google Workspace.

Examples include Backupify, Spanning Backup, and Afi.ai.

Choose a Suitable Tool: Based on your organization's needs and compliance requirements, select a tool that offers robust data retention, secure storage, and easy recovery options.

Set Up the Backup Solution:

Create an Account: Sign up for the chosen third-party backup service.

Configure Backup Settings: Link your Google Workspace account and configure the backup settings to meet your data retention policies.

Schedule Backups: Set up regular backup schedules to ensure data is continuously backed up.

Test Backups and Recovery: Perform initial backups and test the recovery process to ensure data can be retrieved efficiently when needed.

Monitor and Maintain: Regularly monitor the backup status and maintain the system to comply with your organization's data retention regulations.

Reference

Google Workspace Admin Help - Choose a third-party backup tool

Backupify - Google Workspace Backup

• • • • •

Google-Workspace-Administrator Certification Dumps: <https://www.pass4suresvce.com/Google-Workspace-Administrator-pass4sure-vce-dumps.html>

- 2025 Latest Pass4suresVCE Google-Workspace-Administrator PDF Dumps and Google-Workspace-Administrator Exam Engine
Free Share: https://drive.google.com/open?id=1NHu3cz7B6fTHWBd4UNxgrw1Hf_He6Dym