

Google.Google-Workspace-Administrator.v2023-03-13.q55

Exam Code:	Google-Workspace-Administrator
Exam Name:	Google Cloud Certified - Professional Google Workspace Administrator
Certification Provider:	Google
Free Question Number:	55
Version:	v2023-03-13
# of views:	916
# of Questions views:	550
https://www.freepdfdumps.com/Google.Google-Workspace-Administrator.v2023-03-13.q55.html	

NEW 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)

Answer: B (LEAVE A REPLY)

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>

NEW QUESTION: 2

A user is reporting that external, inbound messages from known senders are repeatedly being incorrectly classified as spam. What steps should the admin take to prevent this behavior in the future?

- A. Modify the SPF record for your internal domain to include the IPs of the external user's mail servers.
- B. Update the spam settings in the Admin Console to be less aggressive.
- C. Add the sender's domain to an allowlist via approved senders in the Admin Console.
- D. Instruct the user to add the senders to their contacts.

Answer: C (LEAVE A REPLY)

<https://support.google.com/a/answer/60752?hl=en#:~:text=Approved%20senders%20list%E2%80%94,settings%20in%20Google%20Workspace.>

NEW QUESTION: 3

In the years prior to your organization moving to Google Workspace, 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 Google Workspace.) 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-Google Workspace 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 Google Workspace and Other Google Services disabled.

Answer: (SHOW ANSWER)

<https://support.google.com/a/answer/6178640?hl=en>

NEW QUESTION: 4

Your-company.com recently started using Google Workspace. The CIO is happy with the deployment, but received notifications that some employees have issues with consumer Google accounts (conflict accounts). You want to put a plan in place to address this concern.

What should you do?

- A. Use the conflict account remove tool to remove the accounts from Google Workspace.
- B. Rename the accounts to temp@your-company.com, and recreate the accounts.
- C. Ask users to request a new Google Workspace account from your local admin.
- D. Use the Transfer tool for unmanaged users to find the conflict accounts.

Answer: (SHOW ANSWER)

<https://gsuiteupdates.googleblog.com/2017/02/resolve-conflicting-accounts-with-new.html#:~:text=Using%20the%20new%20Transfer%20tool,accounts%20to%20G%20Suite%20accounts.> <https://support.google.com/a/answer/6178640?hl=en>

NEW QUESTION: 5

A user reached out to the IT department about a Google Group that they own: info@company.com. The group is receiving mail, and each message is also delivered directly to the user's Gmail inbox. The user wants to be able to reply to messages directly from Gmail and have them sent on behalf of the group, not their individual account. Currently, their replies come from their individual account. What would you instruct the user to do?

- A.** Create a new content compliance rule that matches the user's outgoing messages with the group copied, and have it modify the sender to be the group address.
- B.** Add the group as an email address that can be sent from within Gmail, and verify that the user has access. They can then choose to reply from the group.
- C.** Add the user's individual account as a delegate to the group's inbox. They can then toggle between the accounts and use the Gmail interface on behalf of the group.
- D.** Set the group address to be the default sender within the group's posting policies.

Answer: B (LEAVE A REPLY)

<https://support.google.com/googlecloud/answer/10635789?hl=en>

NEW QUESTION: 6

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.

Answer: (SHOW ANSWER)

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.

NEW QUESTION: 7

Your organization's information security team has asked you to determine and remediate if a user (user1@example.com) has shared any sensitive documents outside of your organization. How would you audit access to documents that the user shared inappropriately?

- A. Open Security Investigation Tool-> Drive Log Events. Add two conditions: Visibility Is External, and Actor Is user1@example.com.
- B. Have the super administrator use the Security API to audit Drive access.
- C. As a super administrator, change the access on externally shared Drive files manually under user1@example.com.
- D. Open Security Dashboard-> File Exposure Report-> Export to Sheet, and filter for user1@example.com.

Answer: A (LEAVE A REPLY)

https://support.google.com/a/answer/11480192?hl=en&ref_topic=11479095#:~:text=View%20files%20shared,Click%20Search.

NEW QUESTION: 8

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 Google Workspace admin.
- B. The Apps Script will need to run on a timed interval to process new entries.
- C. The Google Form will need to be limited to internal users only.
- D. The Google Form will need to enforce Group naming conventions.
- E. You will need a Cloud SQL instance to store "G-Team" data.

Answer: (SHOW ANSWER)

NEW QUESTION: 9

A user is reporting that after they sign in to Gmail, their labels are not loading and buttons are not responsive. What action should you take to troubleshoot this issue with the user?

- A. Check whether traceroute to service.gmail.com (pop.gmail.com or imap.gmail.com) is successful.
- B. Check whether a ping test to service.gmail.com (pop.gmail.com or imap.gmail.com) is successful.
- C. Collect full message headers for examination.
- D. Check whether the issue occurs when the user authenticates on a different device or a new incognito window.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 10

In your organization, users have been provisioned with either Google Workspace Enterprise, Google Workspace Business, or no license, depending on their job duties, and

the cost of user licenses is paid out of each division's budget. In order to effectively manage the license disposition, team leaders require the ability to look up the type of license that is currently assigned, along with the last logon date, for their direct reports. You have been tasked with recommending a solution to the Director of IT, and have gathered the following requirements:

Team leaders must be able to retrieve this data on their own (i.e., self-service).

Team leaders are not permitted to have any level of administrative access to the Google Workspace Admin panel.

Team leaders must only be able to look up data for their direct reports.

The data must always be current to within 1 week.

Costs must be mitigated.

What approach should you recommend?

- A. Export log data to BigQuery with custom scopes.
- B. Use a third-party tool.
- C. Use App Script and filter views within a Google Sheet.
- D. Create an app using AppMaker and App Script.

Answer: (SHOW ANSWER)

<https://support.google.com/a/answer/9682494?hl=en>

NEW QUESTION: 11

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.

Answer: D (LEAVE A REPLY)

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

NEW QUESTION: 12

Your organization is about to expand by acquiring two companies, both of which are using Google Workspace. The CISO has mandated that strict 'No external content sharing' policies must be in place and followed. How should you securely configure sharing policies

to satisfy both the CISO's mandate while allowing external sharing with the newly acquired companies?

- A. Allow external sharing of Drive content for the IT group only.
- B. Create a Drive DLP policy that will allow sharing to only domains on an allowlist.
- C. Use shared drives to store the content, and share only individual files externally.
- D. Let users share files between the two companies by using the 'Trusted Domains' feature. Create an allowlist of the trusted domains, and choose sharing settings for the users.

Answer: (SHOW ANSWER)

<https://support.google.com/a/answer/6160020?hl=en#zippy=%2Cgive-sharing-access-to-trusted-domains:~:text=only%20trusted%20domains-,Allow%20external%20sharing%20with%20only%20trusted%20domains,-Help%20and%20tips>

NEW QUESTION: 13

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.

Answer: C (LEAVE A REPLY)

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

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

NEW QUESTION: 14

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

Answer: C (LEAVE A REPLY)

<https://cloud.google.com/solutions/partners/backing-up-g-suite-data-with-spinbackup>

NEW QUESTION: 15

The CEO of your company has indicated that messages from trusted contacts are being delivered to spam, and it is significantly affecting their work. The messages from these contacts have not always been classified as spam. Additionally, you recently configured SPF, DKIM, and DMARC for your domain. You have been tasked with troubleshooting the issue.

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

- A. Validate that your domain is not on the Spamhaus blacklist.
- B. Set up a Gmail routing rule to whitelist the sender.
- C. Conduct an Email log search to trace the message route.
- D. Review the contents of the messages in Google Vault.
- E. Obtain the message header and analyze using Google Workspace Toolbox.

Answer: B,E (LEAVE A REPLY)

NEW QUESTION: 16

Your Accounts Payable department is auditing software license contracts companywide and has asked you to provide a report that shows the number of active and suspended users by organization unit, which has been set up to match the Regions and Departments within your company. You need to produce a Google Sheet that shows a count of all active user accounts and suspended user accounts by Org unit.

What should you do?

- A. From the Admin Console Billing Menu, turn off auto-assign, and then click into Assigned Users and export the data to Sheets.
- B. From the Admin Console Users Menu, download a list of all Users to Google Sheets, and join that with a list of ORGIDs pulled from the Reports API.
- C. From the Google Workspace Reports Menu, run and download the Accounts Aggregate report, and export the data to Google Sheets.
- D. From the Admin Console Users Menu, download a list of all user info columns and currently selected columns.

Answer: D (LEAVE A REPLY)

<https://support.google.com/a/answer/7348070?hl=it>

Valid Google-Workspace-Administrator Dumps shared by Actual4test.com for Helping Passing Google-Workspace-Administrator Exam! Actual4test.com now offer the **newest Google-Workspace-Administrator exam dumps**, the Actual4test.com Google-Workspace-Administrator exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com Google-Workspace-Administrator dumps with Test Engine here: <https://www.actual4test.com/Google->

NEW QUESTION: 17

Your company moved to Google Workspace last month and wants to install Hangouts Meet Hardware in all of their conference rooms. This will allow employees to walk into a room and use the in-room hardware to easily join their scheduled meeting. A distributed training session is coming up, and the facilitator wants to make remote room joining even easier. Participants in remote rooms should walk into their room and begin receiving the training without having to take any actions to join the session.

How should you accomplish this?

- A. In the Admin Console, select the devices in Meeting Room Hardware, select Call, and Enter the meeting code.
- B. Room participants will need to start the meeting from the remote in the room.
- C. By adding the rooms to the Calendar invite, they will all auto-join at the scheduled time.
- D. Select Add Live Stream to the Calendar invite; all rooms added to the event will auto-join at the scheduled time.

Answer: A (LEAVE A REPLY)

<https://support.google.com/meethardware/answer/6069329>

NEW QUESTION: 18

Madeupcorp.com is in the process of migrating from a third-party email system to Google Workspace. The VP of Marketing is concerned that her team already administers the corporate AdSense, AdWords, and YouTube channels using their @madeupcorp.com email addresses, but has not tracked which users have access to which service. You need to ensure that there is no disruption.

What should you do?

- A. Run the Transfer Tool for Unmanaged users.
- B. Use a Google Form to survey the Marketing department users.
- C. Assure the VP that there is no action required to configure Google Workspace.
- D. Contact Google Enterprise Support to identify affected users.

Answer: (SHOW ANSWER)

<https://support.google.com/a/answer/7062710>

NEW QUESTION: 19

Your Chief Information Security Officer is concerned about phishing. You implemented 2 Factor Authentication and forced hardware keys as a best practice to prevent such attacks. The CISO is curious as to how many such email phishing attempts you've avoided since putting the 2FA+Hardware Keys in place last month.

Where do you find the information your CISO is interested in seeing?

- A. Security > Advanced Security Settings > Phishing Attempts

- B. Apps > Google Workspace > Gmail > Phishing Attempts
- C. Security > Dashboard > Spam Filter: Phishing
- D. Reporting > Reports > Phishing

Answer: ([SHOW ANSWER](#))

<https://support.google.com/a/answer/7491892?hl=en>

NEW QUESTION: 20

A retail company has high employee turnover due to the cyclical nature in the consumer space. The increase in leaked confidential content has created the need for a specific administrative role to monitor ongoing employee security investigations. What step should you take to increase the visibility of such investigations?

- A. Create a 'Custom Role' and add the ability to manage Google Vault matters, holds, searches, and exports.
- B. Validate that the new administrator has access to Google Vault.
- C. Create a 'Custom Role' and add all the Google Vault privileges for a new administrator.
- D. Assign the 'Services Admin' role to an administrator with 'Super Admin' privileges.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 21

Your company is using Google Workspace Enterprise Plus, and the Human Resources (HR) department is asking for access to Work Insights to analyze adoption of Google Workspace for all company employees. You assigned a custom role with the work Insights permission set as "view data for all teams" to the HR group, but it is reporting an error when accessing the application. What should you do?

- A. Confirm that the Work Insights app is turned ON for all employees.
- B. Confirm in Security > API controls > App Access Controls that Work Insights API is set to "unrestricted."
- C. Confirm in Reports > BigQuery Export that the job is enabled.
- D. Allocate the "view data for all teams" permission to all employees of the company.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 22

Your organization has enabled spoofing protection against unauthenticated domains. You are receiving complaints that email from multiple partners is not being received. While investigating this issue, you find that emails are all being sent to quarantine due to the configured safety setting. What should be the next step to allow users to review these emails and reduce the internal complaints while keeping your environment secure?

- A. Add your partner domains IPs to the Inbound Gateway setting.
- B. Change the spoofing protection to deliver the emails to spam instead of quarantining them.
- C. Add your partner sending IP addresses to an allowlist.

D. Change the spoofing protection to deliver the emails to inboxes with a custom warning instead of quarantining them.

Answer: B (LEAVE A REPLY)

<https://support.google.com/a/answer/9157861?hl=en#:~:text=Move%20email%20to,with%20this%20action.>

NEW QUESTION: 23

Your organization has noticed several incidents of accidental oversharing inside the organization. Specifically, several users have shared sensitive Google Drive items with the entire organization by clicking 'anyone in this group with this link can view'. You have been asked by senior management to help users share more appropriately and also to prevent accidental oversharing to the entire organization. How would you best accomplish this?

A. Create groups, add users accordingly, and educate users on how to share to specific groups of people.

B. Disable sharing to the entire organization so that users must consciously add every person who needs access.

C. Determine sharing boundaries for users that work with sensitive information, and then implement target audiences.

D. Temporarily disable the Google Drive service for individuals who continually overshare.

Answer: (SHOW ANSWER)

<https://support.google.com/a/answer/9934697?hl=en#zippy=:~:text=Why%20use%20target,for%20broad%20sharing.>

NEW QUESTION: 24

Your organization syncs directory data from Active Directory to Google Workspace 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 Google Workspace Admin panel.

B. Change the user's primary email address in the Google Workspace Admin panel.

C. Change the user's last name in the Google Workspace Admin panel.

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

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

Answer: D,E (LEAVE A REPLY)

<https://support.google.com/a/answer/106368?hl=en>

NEW QUESTION: 25

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.

Answer: D (LEAVE A REPLY)

<https://support.google.com/a/answer/3540538?hl=en>

NEW QUESTION: 26

You act as the Google Workspace Administrator for a company that has just acquired another organization. The acquired company will be migrated into your Workspace environment in 6 months. Management has asked you to ensure that the Google Workspace users you currently manage can efficiently access rich contact information in Workspace for all users. This needs to occur before the migration, and optimally without additional expenditure. What step do you take to populate contact information for all users?

- A.** Bulk-upload the contact information for these users via CSV into the Google Directory.
- B.** Use the Domain Shared Contacts API to upload contact information for the acquired company's users.
- C.** Provision and license Google Workspace accounts for the acquired company's users because they will need accounts in the future.
- D.** Prepare an uploadable file to be distributed to your end users that allows them to add the acquired company's user contact information to their personal contacts.

Answer: (SHOW ANSWER)

The Domain Shared Contacts API lets your applications get and update external contacts that are shared with all users in a Google Workspace domain. Shared contacts are visible to all users of a Google Workspace domain and all Google services have access to the contact list <https://developers.google.com/admin-sdk/domain-shared-contacts/overview>

NEW QUESTION: 27

What steps does an administrator need to take to enforce TLS with a particular domain?

- A.** Enable email safety features with the receiving domain.
- B.** Set up secure transport compliance with the receiving domain.

C. Configure an alternate secure route with the receiving domain.

D. Set up DKIM authentication with the receiving domain.

Answer: B (LEAVE A REPLY)

[https://support.google.com/a/answer/2520500?hl=en#:~:text=Add%20the%20Secure%20transport%20\(TLS\)%20compliance%20setting%20to%20always%20use%20TLS%20for%20email%20sent%20to%20and%20from%20domains%20and%20addresses%20that%20you%20specify.](https://support.google.com/a/answer/2520500?hl=en#:~:text=Add%20the%20Secure%20transport%20(TLS)%20compliance%20setting%20to%20always%20use%20TLS%20for%20email%20sent%20to%20and%20from%20domains%20and%20addresses%20that%20you%20specify.)

NEW QUESTION: 28

Your organization does not allow users to share externally. The security team has recently approved an exemption for specific members of the marketing team and sales to share documents with external customers, prospects, and partners. How best would you achieve this?

A. Create a configuration group with the approved users as members, and use it to create a target audience.

B. Enable external sharing for the marketing and sales organizational units.

C. Enable external sharing only to allowlisted domains provided by marketing and sales teams.

D. Create a configuration group with the approved users as members, and enable external sharing for this group.

Answer: D (LEAVE A REPLY)

<https://support.google.com/a/answer/9224126?hl=en#zippy=%2Coptions-for-configurations-groups:~:text=Using%20configurations%20groups,of%20your%20organization.>

NEW QUESTION: 29

Your company is deploying Chrome devices. You want to make sure the machine assigned to the employee can only be signed in to by that employee and no one else.

What two things should you do? (Choose two.)

A. Disable Guest Mode and Public Sessions.

B. Enable a Device Policy of Sign In Screen and add the employee email address.

C. Enroll a 2-Factor hardware key on the device using the employee email address.

D. Enable a User Policy of Multiple Sign In Access and add just the employee email address.

E. Enable a Device Policy of Restrict Sign In to List of Users, and add the employee email address.

Answer: A,E (LEAVE A REPLY)

<https://support.google.com/chrome/a/answer/1375678?hl=en>

NEW QUESTION: 30

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.** Under Drive and Docs > Sharing Settings, the "Whitelisted domains" list needs to be updated to add the new ISP domain.
- B.** You need to raise a ticket to Google Cloud Support to have your new IP ranges registered for Drive API access.
- C.** An access level was defined based on the IP range and applied to Google Drive via Context-Aware Access.
- D.** The Network Mask defined in Security > Settings > SSO with 3rd Party IdPs should be updated to reflect the new IP range.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 31

Your business partner requests that a new custom cloud application be set up to log in without having separate credentials.

What is your business partner required to provide in order to proceed?

- A.** Service provider logout URL
- B.** Service provider ACS URL
- C.** Identity Provider URL
- D.** Service provider certificate

Answer: B (LEAVE A REPLY)

Reference:

we need ACS URL for adding custom SAML App , using Google as the Idp

Valid Google-Workspace-Administrator Dumps shared by Actual4test.com for Helping Passing Google-Workspace-Administrator Exam! Actual4test.com now offer the **newest Google-Workspace-Administrator exam dumps**, the Actual4test.com Google-Workspace-Administrator exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com Google-Workspace-Administrator dumps with Test Engine here: https://www.actual4test.com/Google-Workspace-Administrator_examcollection.html (103 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

NEW QUESTION: 32

Your organization has a new security requirement around data exfiltration on iOS devices. You have a requirement to prevent users from copying content from a Google app (Gmail, Drive, Docs, Sheets, and Slides) in their work account to a Google app in their personal account or a third-party app. What steps should you take from the admin panel to prevent users from copying data from work to non-work apps on iOS devices?

- A.** Navigate to "Data Protection" setting in Google Admin Console's Device management section and disable the "Allow users to copy data to personal apps" checkbox.
- B.** Disable "Open Docs in Unmanaged Apps" setting in Google Admin Console's Device management section.
- C.** Navigate to Devices > Mobile and endpoints > Universal Settings > General and turn on Basic Mobile Management.
- D.** Clear the "Allow items created with managed apps to open in unmanaged apps" checkbox.

Answer: A (LEAVE A REPLY)

[https://support.google.com/a/answer/6328700?](https://support.google.com/a/answer/6328700?hl=en&ref_topic=6079327#managed_apps&zippy=%2Cdata-actions)

[hl=en&ref_topic=6079327#managed_apps&zippy=%2Cdata-actions](https://support.google.com/a/answer/6328700?hl=en&ref_topic=6079327#managed_apps&zippy=%2Cdata-actions) Allow users to copy Google Workspace items to personal apps Allows users to copy content from a Google app (such as Gmail, Drive, Docs, Sheets, Slides, Chat, and Meet) to a Google app in their personal account or a third-party app. Also allows users to drag content between Google apps, for any account.

To prevent users from copying or dragging information from their work account, or using the All inboxes feature (which combines messages from multiple Gmail accounts into one inbox), uncheck the box.

NEW QUESTION: 33

The application development team has come to you requesting that a new, internal, domain-owned Google Workspace 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.** Add OAuth Client ID to Google Drive Trusted List.
- B.** Enable all API access for Google Drive.
- C.** Whitelist the app in the Google Workspace Marketplace.
- D.** Enable "trust domain owned apps" setting.

Answer: (SHOW ANSWER)

NEW QUESTION: 34

Your company's Google Workspace primary domain is "mycompany.com," and it has acquired a startup that is using another cloud provider with a domain named "mystartup.com." You plan to add all employees from the startup to your Google

Workspace domain while preserving their current mail addresses. The startup CEO's email address is andrea@mystartup.com, which also matches your company CEO's email address as andrea@mycompany.com, even though they are different people. Each must keep the usage of their email. In addition, your manager asked to have all existing security policies applied for the new employees without any duplication. What should you do to implement the migration?

- A.** Create a new Google Workspace domain with "mystartup.com," and create a trust between both domains for reusing the same security policies and sharing employee information within the companies.
- B.** Create the startup employees in the "mycompany.com" domain, and add a number at the end of the user name whenever there is a conflict. In Gmail > Routing, define a specific route for the OU that targets the startup employees, which will modify the email address domain to "mystartup.com," and remove any numbers previously added. In addition, confirm that the SPF and DKIM records are properly set.
- C.** Create an alias domain, mystartup.com, in your existing Google Workspace domain, set up necessary DNS records, and create all startup employees with the alias domain as their primary email addresses.
- D.** Create a secondary domain, mystartup.com, within your current Google Workspace domain, set up necessary DNS records, and create all startup employees with the secondary domain as their primary email addresses.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 35

Your company has just received a shipment of ten Chromebooks to be deployed across the company, four of which will be used by remote employees. In order to prepare them for use, you need to register them in Google Workspace.

What should you do?

- A.** In Chrome Management | Device Settings, enable Forced Re-enrollment for all devices.
- B.** Turn on the Chromebook and press Ctrl+Alt+E at the login screen to begin enterprise enrollment.
- C.** Turn on the chromebook and log in as a Chrome Device admin. Press Ctrl+Alt+E to begin enterprise enrollment.
- D.** Instruct the employees to log in to the Chromebook. Upon login, the auto enrollment process will begin.

Answer: **B** ([LEAVE A REPLY](#))

NEW QUESTION: 36

Your company has received help desk calls from users about a new interface in Gmail that they had not seen before. They determined that it was a new feature that Google released recently. In the future, you'll need time to review the new features so you can properly train employees before they see changes.

What action should you take?

- A. Company Profile > Profile > New User Features > Enable "Scheduled Release"
- B. Apps > Google Workspace > Gmail > Uncheck "Enable Gmail Labs for my users"
- C. Company Profile > Profile > New User Features > Enable "Rapid Release"
- D. Device Management > Chrome > Device Settings > Stop auto-updates

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 37

Your organization recently had a sophisticated malware attack that was propagated through embedded macros in email attachments. As a Workspace administrator, you want to provide an additional layer of anti-malware protection over the conventional malware protection that is built into Gmail. What should you do to protect your users from future unknown malware in email attachments?

- A. Run queries in Security Investigation Tool.
- B. Turn on advanced phishing and malware protection.
- C. Enable Security Sandbox.
- D. Enable Gmail confidential mode.

Answer: C ([LEAVE A REPLY](#))

<https://support.google.com/a/answer/7676854?hl=en#zippy=%2Cscan-all-attachments-in-security-sandbox:~:text=detect%20harmful%20attachments-,Set%20up%20rules%20to%20detect%20harmful%20attachments,Security%20Sandbox,-Supported%20editions%20for>

NEW QUESTION: 38

Your company has sales offices in Madrid, Tokyo, London, and New York. The outbound email for those offices needs to include the sales person's signature and a compliance footer. The compliance footer needs to say "Should you no longer wish to receive emails about this offer, please reply with UNSUBSCRIBE." You are responsible for making sure that users cannot remove the footer.

What should you do?

- A. Send an email to each sales person with the instructions on how to add the footer to their Signature.
- B. Ensure that each sales team is in their own OU, and configure the Append Footer with the signature and footer content translated for each locale.
- C. Ensure that each sales team is in their own OU, and configure the Append Footer with footer content.
- D. Ensure that each sales team is in their own OU, and configure the Append Footer with the footer content translated for each locale.

Answer: C ([LEAVE A REPLY](#))

Google Workspace has no way to translate for each region for the footer.

<https://support.google.com/a/answer/2364576?hl=en>

NEW QUESTION: 39

Your organization's Sales Department uses a generic user account (sales@company.com) to manage requests. With only one employee responsible for managing the departmental account, you are tasked with providing the department with the most efficient means to allow multiple employees various levels of access and manage requests from a common email address.

What should you do?

- A. Configure a Google Group as an email list.
- B. Delegate email access to department employees.
- C. Configure a Google Group as a collaborative inbox.
- D. Configure a Google Group, and set the Access Level to Announcement Only.

Answer: (SHOW ANSWER)

<https://support.google.com/a/answer/167430?hl=en>

NEW QUESTION: 40

Your Finance team has to share quarterly financial reports in Sheets with an external auditor. The external company is not a Workspace customer and allows employees to access public sites such as Gmail and Facebook. How can you provide the ability to securely share content to collaborators that do not have a Google Workspace or consumer (Gmail) account?

- A. Allow external sharing with the auditor using the 'Trusted Domains' feature.
- B. Enable the 'Visitor Sharing' feature, and demonstrate it to the Finance team.
- C. Use the 'Publish' feature in the Sheets editor to share the contents externally.
- D. Attach the Sheet file to an email message, and send to the external auditor.

Answer: B (LEAVE A REPLY)

<https://support.google.com/drive/answer/9195194?hl=en#:~:text=Share%20with%20visitors,with%20one%20visitor.>

NEW QUESTION: 41

After making a recent migration to Google Workspace, you updated your Google Cloud Directory Sync configuration to synchronize the global address list. Users are now seeing duplicate contacts in their global directory in Google Workspace. You need to resolve this issue.

What should you do?

- A. Train users to use Google Workspace's merge contacts feature.
- B. Enable directory contact deduplication in the Google Workspace Admin panel.
- C. Update shared contact search rules to exclude internal users.
- D. Create a new global directory, and delete the original.

Answer: (SHOW ANSWER)

<https://support.google.com/a/answer/3075991#duplicatecontacts>

"To resolve this issue, correct your shared contact search rules to exclude users in your own domain. On the next sync, GCDS attempts to delete the redundant contacts. You might need to adjust the shared contact deletion limit for that first sync.

NEW QUESTION: 42

Your employer, a media and entertainment company, wants to provision Google Workspace Enterprise accounts on your domain for several world-famous celebrities. Leadership is concerned with ensuring that these VIPs are afforded a high degree of privacy. Only a small group of senior employees must be able to look up contact information and initiate collaboration with the VIPs using Google Workspace services such as Docs, Chat, and Calendar.

You are responsible for configuring to meet these requirements. What should you do?

- A.** In the Users list, find the VIPs and turn off the User setting "Directory Sharing."
- B.** Create a Group for the VIPs and their handlers, and set the Group Access Level to Restricted.
- C.** In Directory Settings, disable Contact Sharing.
- D.** Create separate Custom Directories for the VIPs and regular employees.

Answer: D (LEAVE A REPLY)

<https://support.google.com/a/answer/7566446?hl=en>

NEW QUESTION: 43

You are in the middle of migrating email from on-premises Microsoft Exchange to Google Workspace. Users that you have already migrated are complaining of messages from internal users going into spam folders. What should you do to ensure that internal messages do not go into Gmail spam while blocking spoofing attempts?

- A.** Train users to click on Not Spam button for emails.
- B.** Add all users of your domain to an approved sender list.
- C.** Force TLS for your domain.
- D.** Ensure that your inbound gateway is configured with all of your Exchange server IP addresses.

Answer: B (LEAVE A REPLY)

Approved senders list-Approved senders are trusted users that send email to your organization. Create an address list of approved senders so messages from these users bypass Gmail's spam filters, and recipients can decide whether they are spam or not. Create the list with individual email addresses, or by adding an entire domain.

<https://support.google.com/a/answer/60752?hl=en#:~:text=Approved%20senders%20list%E2%80%94,settings%20in%20Google%20Workspace.>

NEW QUESTION: 44

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.

Answer: (SHOW ANSWER)

Randomly scatter auto-updates over Only available if you choose to scatter updates Specifies the approximate number of days that managed Chrome devices download an update after its release. You can use this setting to avoid causing traffic spikes in old or low-bandwidth networks. Devices that are offline during this period download the update when they're online again. <https://support.google.com/chrome/a/answer/1375678?hl=en#zippy=%2Cauto-update-settings>

NEW QUESTION: 45

Your organization has implemented Single Sign-On (SSO) for the multiple cloud-based services it utilizes. During authentication, one service indicates that access to the SSO provider cannot be accessed due to invalid information.

What should you do?

- A. Verify the NameID Element in the SAML Response matches the Assertion Consumer Service (ACS) URL.
- B. Verify the Audience Element in the SAML Response matches the Assertion Consumer Service (ACS) URL.
- C. Verify the Subject attribute in the SAML Response matches the Assertion Consumer Service (ACS) URL.
- D. Verify the Recipient attribute in the SAML Response matches the Assertion Consumer Service (ACS) URL.

Answer: (SHOW ANSWER)

Reference:

<https://support.google.com/a/answer/2463723?hl=en>

NEW QUESTION: 46

Your company has acquired a new company in Japan and wants to add all employees of the acquisition to your existing Google Workspace domain. The new company will retain its original domain for email addresses and, due to the very sensitive nature of its work, the new employees should not be visible in the global directory. However, they should be visible within each company's separate directory. What should you do to meet these requirements?

- A.** Create a new Google Workspace domain isolated from the existing one, and create users in the new domain instead.
- B.** Under Directory Settings > Contact sharing, disable the contact sharing option and wait for 24 hours to allow the settings to propagate before creating the new employee accounts.
- C.** Redesign your OU organization to have 2 child OUs for each company directly under the root. In Directory Settings > Visibility Settings, define custom directories for each company, and set up Visibility according to the OU.
- D.** Create one dynamic group for each company based on a custom attribute defining the company. In Directory Settings > Visibility Settings, define custom directories for each company, and set up Visibility according to the dynamic group.

Answer: ([SHOW ANSWER](#))

https://support.google.com/a/answer/7566446?hl=en&ref_topic=9832541

Valid Google-Workspace-Administrator Dumps shared by Actual4test.com for Helping Passing Google-Workspace-Administrator Exam! Actual4test.com now offer the **newest Google-Workspace-Administrator exam dumps**, the Actual4test.com Google-Workspace-Administrator exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com Google-Workspace-Administrator dumps with Test Engine here: https://www.actual4test.com/Google-Workspace-Administrator_examcollection.html (103 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

NEW QUESTION: 47

What action should be taken to configure alerting related to phishing attacks?

- A.** Set up an email settings changed alert.
- B.** Set up a suspicious login event alert.
- C.** Set up an Admin audit log event alert.
- D.** Set up a Token audit log event alert.

Answer: **B** ([LEAVE A REPLY](#))

NEW QUESTION: 48

Security and Compliance has identified secure third-party applications that should have access to Google Workspace data. You need to restrict third-party access to only approved applications. What two actions should you take? (Choose two.)

- A.** Restrict API scopes
- B.** Disable the Drive SDK
- C.** Disable add-ons for Gmail
- D.** Whitelist Trusted Apps
- E.** Whitelist Google Workspace Marketplace apps

Answer: A,D ([LEAVE A REPLY](#))

NEW QUESTION: 49

On which two platforms can you push WiFi connection information with Google Workspace? (Choose two.)

- A. Mac OS
- B. iOS
- C. Windows
- D. Linux
- E. Chrome OS

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 50

You are a Workspace Administrator with a mix of Business Starter and Standard Licenses for your users. A Business Starter User in your domain mentions that they are running out of Drive Storage Quota. Without deleting data from Drive, what two actions can you take to alleviate the quota concerns for this user? (Choose two.)

- A. Make another user the "Owner" of the Drive objects, thus transferring the storage quota debt to them.
- B. Add other users as "Editors" on the Drive object, thus spreading the storage quota debt between all of them.
- C. Perform an API query for large storage drive objects, and delete them, thus alleviating the quota debt.
- D. Move the affected items to a Shared Drive. Shared Drives transfer ownership of the drive item to the domain itself, which alleviates the quota debt from that user.
- E. Manually export and back up the data locally, and delete the affected files from Drive to alleviate the debt.

Answer: A,D ([LEAVE A REPLY](#))

NEW QUESTION: 51

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 Google Workspace 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 Google Workspace 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 Google Workspace support forum for feedback about the app to include in the risk analysis report.

Answer: (SHOW ANSWER)

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

NEW QUESTION: 52

Your organization wants more visibility into actions taken by Google staff related to your data for audit and security reasons. They are specifically interested in understanding the actions performed by Google support staff with regard to the support cases you have opened with Google. What should you do to gain more visibility?

- A.** From Google Admin Panel, go to Audit, and select Access Transparency Logs. Most Voted
- B.** From Google Admin Panel, go to Audit, and select Login Audit Log.
- C.** From Google Admin Panel, go to Audit, and select Rules Audit Log.
- D.** From Google Admin Panel, go to Audit, and select Admin Audit Log.

Answer: A (LEAVE A REPLY)

Google staff logs related to accessing user content are stored in Access Transparency logs <https://support.google.com/a/answer/9230474?hl=en>

NEW QUESTION: 53

A company using Google Workspace has reports of cyber criminals trying to steal usernames and passwords to access critical business data. You need to protect the highly sensitive user accounts from unauthorized access.

What should you do?

- A.** Turn on password expiration.
- B.** Enforce 2FA with a physical security key.
- C.** Use a third-party identity provider.
- D.** Enforce 2FA with Google Authenticator app.

Answer: B (LEAVE A REPLY)

<https://support.google.com/a/answer/175197?hl=en#keys&prompt&authentic&codes&phone&2sv&security>

NEW QUESTION: 54

Your IT team is being asked to fulfill a query by your organization's legal department that requires an MBOX file that will be shared to a third-party partner for eDiscovery. The query

must be run on multiple users. Legal has no admin rights to Google Vault. What should you do to fulfil the request?

- A.** Create a Google Vault matter for each user account, and share the matters to the legal admin.
- B.** Create a Google Vault matter, search for data, and run an export for the legal department.
- C.** Use the Investigation Tool to search for the data requested, and export for the legal department.
- D.** Search for the data in Gmail, and export for the legal department.

Answer: B (LEAVE A REPLY)

<https://support.google.com/vault/answer/2473458?hl=en>

NEW QUESTION: 55

Your sales team, which is organized as its own organizational unit, is prone to receiving malicious attachments. What action should you take, as an administrator, to apply an additional layer of protection in the admin console for your sales team without disrupting business operation?

- A.** Configure an attachment compliance rule to send any emails with attachments received by users within the sales team organizational unit to an administrator quarantine.
- B.** Configure an attachment compliance rule to strip any attachments received by users within the sales team organizational unit.
- C.** Configure the security sandbox feature on the sales team organizational unit.
- D.** Update the Email Allowlist in the admin console to only include IP addresses of known senders.

Answer: C (LEAVE A REPLY)

<https://support.google.com/a/answer/7676854?hl=en#:~:text=As%20an%20administrator,malicious%20attachments.>

Valid Google-Workspace-Administrator Dumps shared by Actual4test.com for Helping Passing Google-Workspace-Administrator Exam! Actual4test.com now offer the **newest Google-Workspace-Administrator exam dumps**, the Actual4test.com Google-Workspace-Administrator exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com Google-Workspace-Administrator dumps with Test Engine here: https://www.actual4test.com/Google-Workspace-Administrator_examcollection.html (103 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)