



**Vendor:** Google

**Exam Code:** Google-Workspace-Administrator

**Exam Name:** Professional Google Workspace Administrator

**Version:** DEMO

### QUESTION 1

As the Workspace Administrator, you have been asked to configure Google Cloud Directory Sync (GCDS) in order to manage Google Group memberships from an internal LDAP server. However, multiple Google Groups must have their memberships managed manually. When you run the GCDS sync, you notice that these manually managed groups are being deleted. What should you do to prevent these groups from being deleted?

- A. In the GCDS configuration manager, update the group deletion policy setting to "don't delete Google groups not found in LDAP."
- B. Use the Directory API to check and update the group's membership after the GCDS sync is completed.
- C. Confirm that the base DN for the group email address attribute matches the base DN for the user email address attribute.
- D. In the user attribute settings of the GCDS configuration manager options, set the Google domain users deletion/suspension policy to "delete only active Google domain users not found in LDAP."

**Answer: A**

**Explanation:**

Don't delete Google Groups not found in LDAP If checked, Google Group deletions in your Google domain are disabled, even when the Groups aren't in your LDAP server.

<https://support.google.com/a/answer/6258071?hl=en#zippy=%2Cgoogle-group-deletion-policy>

### QUESTION 2

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**

**Explanation:**

[https://support.google.com/a/answer/6328700?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.

### QUESTION 3

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: C**

**Explanation:**

<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.

#### QUESTION 4

The company's ten most senior executives are to have their offices outfitted with dedicated, standardized video conference cameras, microphones, and screens. The goal is to reduce the amount of technical support they require due to frequent, habitual switching between various mobile and PC devices throughout their busy days. You must ensure that it is easier for the executives to join Meet video conferences with the dedicated equipment instead of whatever device they happen to have available.

What should you do?

- A. Set up unmanaged Chromeboxes and set the executives' homepage to meet.google.com via Chrome settings.
- B. Set up the executive offices as reservable Calendar Resources, deploy Hangouts Meet Hardware Kits, and associate the Meet hardware with the room calendars.
- C. Deploy Hangouts Meet Hardware Kits to each executive office, and associate the Meet hardware with the executives' calendars.
- D. Provision managed Chromeboxes and set the executives' Chrome homepage to meet.google.com via device policy.

**Answer: C**

**Explanation:**

<https://support.google.com/meethardware/answer/3341435?hl=en>

If the device is for a single user, such as in a home office or other remote location, you can associate the device with their personal calendar. Whenever an organizer adds that user to a Calendar event, the meeting name appears on their device.

#### QUESTION 5

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: A**

**Explanation:**

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.

Reference:

<https://support.google.com/chrome/a/answer/1375678?hl=en#zippy=%2Cauto-update-settings>

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

**QUESTION 6**

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**

**Explanation:**

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

Reference:

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

**QUESTION 7**

Your organization is concerned with the increasing threat of phishing attacks that may impact users. Leadership has declined to force-enable 2-Step verification.

You need to apply a security measure to prevent unauthorized access to user accounts.

What should you do?

- A. Enable Enforce Strong Password policy.
- B. Enable Employee ID Login Challenge.
- C. Decrease the Maximum User Session Length.
- D. Revoke token authorizations to external applications.

**Answer: B**

**Explanation:**

You can use employee IDs as a login challenge. Employee IDs are more difficult to guess and

phish than other types of identity challenges. To use the employee ID login challenge, you need to make sure that IDs are associated with your users' accounts.  
<https://support.google.com/a/answer/6002699?hl=en>

#### QUESTION 8

Your company (your-company.com) just acquired a new business (new-company.com) that is running their email on-premises. It is close to their peak season, so any major changes need to be postponed. However, you need to ensure that the users at the new business can receive email addressed to them using your-company.com into their on-premises email server. You need to set up an email routing policy to accomplish this.

What steps should you take?

- A. Set up an Outbound Mail Gateway to route all outbound email to the on-premises server.
- B. Set up accounts for the new employees, and use mail forwarding rules to send to the on-premises server.
- C. Set up an Inbound Mail Gateway to reroute all inbound email to the on-premises server.
- D. Set up a Default route with split delivery to route email to the on-premises server.

**Answer: D**

**Explanation:**

<https://support.google.com/a/answer/2685650?hl=en>

"...If you're migrating to Gmail from a legacy server, use split delivery to test Gmail with a subset of users. During the testing, the MX records for your domain point to Gmail. Users who have been added in the Admin console get messages in their Gmail inboxes. Set up a catch-all routing rule for unregistered users who need to get messages from the legacy mail server."

#### QUESTION 9

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: 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 10

Your company has an OU that contains your sales team and an OU that contains your market research team. The sales team is often a target of mass email from legitimate senders, which is distracting to their job duties. The market research team also receives that email content, but they want it because it often contains interesting market analysis or competitive intelligence. Constant Contact is often used as the source of these messages. Your company also uses Constant Contact for your own mass email marketing. You need to set email controls at the Sales OU

without affecting your own outgoing email or the market research OU.

What should you do?

- A. Create a blocked senders list as the Sales OU that contains the mass email sender addresses, but bypass this setting for Constant Contact emails.
- B. Create a blocked senders list at the root level, and then an approved senders list at the Market Research OU, both containing the mass email sender addresses.
- C. Create a blocked senders list at the Sales OU that contains the mass email sender addresses.
- D. Create an approved senders list at the Market Research OU that contains the mass email sender addresses.

**Answer: C**

**Explanation:**

"The sales team is often a target of mass email from legitimate senders, which is distracting to their job duties" and "Constant Contact is often used as the source of these messages". Nowhere in the question did it specify that emails received via Constant Contact should be allowed for the sales OU. It only mentioned that the company uses Constant Contact for its own outgoing emails- which in this case does not affect the answer at all.

#### QUESTION 11

Your company recently decided to use a cloud-based ticketing system for your customer care needs. You are tasked with rerouting email coming into your customer care address, [customercare@your-company.com](mailto:customercare@your-company.com) to the cloud platform's email address, [your-company@cloudprovider.com](mailto:your-company@cloudprovider.com). As a security measure, you have mail forwarding disabled at the domain level.

What should you do?

- A. Create a mail contact in the Google Workspace directory that has an email address of [your-company@cloudprovider.com](mailto:your-company@cloudprovider.com)
- B. Create a rule to forward mail in the [customercare@your-company.com](mailto:customercare@your-company.com) mailbox to [your-company@cloudprovider.com](mailto:your-company@cloudprovider.com)
- C. Create a recipient map in the Google Workspace Admin console that maps [customercare@your-company.com](mailto:customercare@your-company.com) to [your-company@cloudprovider.com](mailto:your-company@cloudprovider.com)
- D. Create a content compliance rule in the Google Workspace Admin console to change route to [your-company@cloudprovider.com](mailto:your-company@cloudprovider.com)

**Answer: C**

**Explanation:**

Disable automatic forwarding <https://support.google.com/a/answer/2491924?hl=en>

Redirect incoming messages to another email address

<https://support.google.com/a/answer/4524505?hl=en>

(Optional) To send the message to the original recipient as well as the new address, under Routing options, check the Also route to original destination box.

#### QUESTION 12

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.

**Answer: A**

**Explanation:**

Login audit log Track user sign-in activity You can use the Login audit log to track user sign-ins to your domain. You can review all sign-ins from web browsers. If a user signs in from an email client or a non-browser application, you can only review reports of suspicious attempts. Forward log event data to the Google Cloud Platform You can opt in to share the log event data with Google Cloud Platform. If you turn on sharing, data is forwarded to Cloud Logging, where you can query and view your logs, and control how you route and store your logs.

<https://support.google.com/a/answer/4580120?hl=en>

### QUESTION 13

The company's ten most senior executives are to have their offices outfitted with dedicated, standardized video conference cameras, microphones, and screens. The goal is to reduce the amount of technical support they require due to frequent, habitual switching between various mobile and PC devices throughout their busy days. You must ensure that it is easier for the executives to join Meet video conferences with the dedicated equipment instead of whatever device they happen to have available.

What should you do?

- A. Set up unmanaged Chromeboxes and set the executives' homepage to meet.google.com via Chrome settings.
- B. Set up the executive offices as reservable Calendar Resources, deploy Hangouts Meet Hardware Kits, and associate the Meet hardware with the room calendars.
- C. Deploy Hangouts Meet Hardware Kits to each executive office, and associate the Meet hardware with the executives' calendars.
- D. Provision managed Chromeboxes and set the executives' Chrome homepage to meet.google.com via device policy.

**Answer: C**

**Explanation:**

<https://support.google.com/meethardware/answer/3341435?hl=en>

If the device is for a single user, such as in a home office or other remote location, you can associate the device with their personal calendar. Whenever an organizer adds that user to a Calendar event, the meeting name appears on their device.



## Thank You for Trying Our Product

### Passleader Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.passleader.com/all-products.html>



Microsoft



ORACLE



JUNIPER  
NETWORKS



EMC²  
where information lives

**10% Discount Coupon Code: ASTR14**



