



- Expert Verified, Online, **Free**.

Madeupcorp.com is in the process of migrating from a third-party email system to G Suite. 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 G Suite.
- D. Contact Google Enterprise Support to identify affected users.

**Suggested Answer: A**

Reference:

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

Community vote distribution

A (100%)

- 🗨️ **szl0144** Highly Voted 2 years, 6 months ago  
took the exam on 5/8/22, only 2 questions here are in the exam, I have to say the dump is not valid anymore. Just want to remind you guys.  
upvoted 5 times
- 🗨️ **Beargoat** 2 years, 1 month ago  
Confirmed - took exam last Friday, totally different questions bar 2 of them.  
upvoted 2 times
- 🗨️ **Jameshaha** Most Recent 1 year, 10 months ago  
Need move to the workspace cert ?  
upvoted 1 times
- 🗨️ **Islam9876** 2 years, 4 months ago  
Anyone who was recently completed the exam  
upvoted 2 times
- 🗨️ **EzraM** 2 years, 6 months ago  
TOOK THE EXAM LAST APRIL 29. THIS QUESTIONNAIRE IS NOT VALID ANYMORE  
upvoted 2 times
- 🗨️ **gfalk85** 2 years, 7 months ago  
Took an exam on April 2022. Exam is totally different from the one listed here!  
upvoted 3 times
- 🗨️ **Sekierer** 2 years, 7 months ago  
Selected Answer: A  
A is correct  
<https://support.google.com/a/answer/7062710>  
upvoted 1 times
- 🗨️ **[Removed]** 2 years, 10 months ago  
Selected Answer: A  
correct answer is A  
upvoted 2 times
- 🗨️ **Ecomunick** 2 years, 10 months ago  
The question here are not update. Still the same as in past.  
upvoted 2 times
- 🗨️ **Trueeye** 2 years, 10 months ago

The exam is totally different from this set.  
Please update the questions with the original exam  
upvoted 4 times

🗨️ 👤 **[Removed]** 2 years, 10 months ago

Hi, in before I could see on Google's website that there are changes to the exam, however it seems that they undo it! do you have any information in this regard? How was the latest exam?  
upvoted 1 times

🗨️ 👤 **Trueeye** 2 years, 10 months ago

@rosafgh : All questions are new.  
upvoted 1 times

🗨️ 👤 **x3lolol** 2 years, 10 months ago

@rosafgh where did you find the google's website regarding the changes? Cause I couldn't see any  
upvoted 1 times

🗨️ 👤 **Kristuc** 3 years, 7 months ago

A is correct  
upvoted 2 times

🗨️ 👤 **saurabh1805** 4 years, 1 month ago

A is correct answer here  
<https://support.google.com/a/answer/7062710>  
upvoted 4 times

🗨️ 👤 **EMO** 4 years, 2 months ago

Vote for A  
upvoted 3 times

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.

**Suggested Answer:** A



Community vote distribution

C (100%)

  **ar18** Highly Voted 4 years ago

I think its C. "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.  
upvoted 13 times

  **Ad99** Most Recent 1 year, 9 months ago

Selected Answer: C

It should be C

upvoted 1 times

  **Dadoks** 2 years, 3 months ago

By passing blocked settings for Constant Contact emails, will still allow mails sent from bulk sender constant contact with a new email address to reach the sales team. Simply blocking the sender email address will still allow internal constant contact mail reach the sales team.

upvoted 1 times

  **miky65** 2 years, 6 months ago

instead in other online sites I have seen that all give the correct answer to A.

upvoted 1 times

  **miky65** 2 years, 6 months ago

Hello, could someone confirm the correct answer please. Thank you


upvoted 1 times

  **[Removed]** 2 years, 10 months ago

Selected Answer: C

correct answer is C

upvoted 2 times

  **RMO000** 2 years, 11 months ago

Selected Answer: C

The Sales OU doesn't need the bypass

upvoted 1 times


  **jcloud965** 3 years ago

**Selected Answer: C**

Why should we bypass the setting for Constant Contact emails ?



Only Sales need to be preserve for inbound mass emailing. This rule will not interfere with their external mass mailing system.

upvoted 2 times

  **ralf\_cc** 3 years, 4 months ago

A - letting the Constant Contact emails, e.g., emails with @constantcontact.com, through will ensure you can still use the service for mass outgoing emails

upvoted 2 times

  **Kristuc** 3 years, 7 months ago



A is correct

upvoted 1 times

  **Twindaddy** 3 years, 8 months ago

I think it's C, too. A blocked senders list containing an exception for Constant Contact would let the very emails you're trying to block right through. You can set up a block rule that doesn't affect outgoing messages.

upvoted 1 times

  **admcloud** 3 years, 10 months ago



Hello, could someone confirm the correct answer please. Thank you

upvoted 3 times

  **saurabh1805** 4 years, 1 month ago


I will go with Option A, you dont want to block those contant contact where you have potential to sell in future,

upvoted 1 times

  **Pakinter** 4 years, 2 months ago


So finally it is A? you can just block for sales OU and create an exception for the specific group.? I think it is the most accurate solution.

upvoted 1 times

  **kerrluis** 4 years, 3 months ago


I would go for A.

upvoted 1 times

  **nwk** 4 years, 5 months ago

Vote for C, 2 different OU, Sales OU setting does not affect Marketing OU

upvoted 4 times

  **HateMicrosoft** 4 years, 3 months ago

<https://support.google.com/a/answer/2364632?hl=en>

upvoted 1 times

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 G Suite 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 G Suite.
- B. Write a script and use G Suite APIs to access and download user data.
- C. Use a third-party tool to configure secure backup of G Suite data.
- D. Train users to use Google Takeout and store their archives locally.

**Suggested Answer: C**

Community vote distribution

C (100%)

🗨️ 👤 **[Removed]** 2 years, 10 months ago

**Selected Answer: C**

correct answer is C

upvoted 1 times

🗨️ 👤 **jcloud965** 3 years ago

Best option should be to use Archived user licence but not listed.

A will only preserve email.

B and C can preserve email and drive.

upvoted 1 times

🗨️ 👤 **Kristuc** 3 years, 7 months ago

C is correct

upvoted 2 times

🗨️ 👤 **felixg27** 3 years, 7 months ago

It's A because this is the most straightforward solution and it doesn't rely on third-party-tools, which would not be considered as best practice. See details about dual-delivery here if you're unaware of that: <https://support.google.com/a/answer/9228551?hl=en>

upvoted 1 times

🗨️ 👤 **felixg27** 3 years, 7 months ago

But honestly I realised now that it depends what is meant by certain G suite data..... My answer would be valid only if they meant mails only

upvoted 1 times

🗨️ 👤 **RMO000** 2 years, 11 months ago

It's wrong because the dual-delivery doesn't do a copy of the previous data.

upvoted 1 times

🗨️ 👤 **saarabh1805** 4 years, 1 month ago

C for me is correct answer, You can use solution like Spinbackup.

upvoted 3 times

🗨️ 👤 **saarabh1805** 4 years, 1 month ago

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

upvoted 2 times

Your organization is on G Suite Enterprise and allows for external sharing of Google Drive files to facilitate collaboration with other G Suite customers. Recently you have had several incidents of files and folders being broadly shared with external users and groups. Your chief security officer needs data on the scope of external sharing and ongoing alerting so that external access does not have to be disabled.

What two actions should you take to support the chief security officer's request? (Choose two.)

- A. Review who has viewed files using the Google Drive Activity Dashboard.
- B. Create an alert from Drive Audit reports to notify of external file sharing.
- C. Review total external sharing in the Aggregate Reports section.
- D. Create a custom Dashboard for external sharing in the Security Investigation Tool.
- E. Automatically block external sharing using DLP rules.

**Suggested Answer:** BE

Community vote distribution

BD (100%)

 **nwk** Highly Voted 4 years, 5 months ago

B and D


[https://support.google.com/a/answer/7584076?hl=en&ref\\_topic=7563358](https://support.google.com/a/answer/7584076?hl=en&ref_topic=7563358)

upvoted 10 times

 **ComputerGirl** Most Recent 2 years, 7 months ago

The expressed a concern with external sharing but did not specify if should be blocked. I agree B for alerts and D for viewing access.

upvoted 1 times

 **Kevin666** 2 years, 9 months ago

B & D is correct

upvoted 1 times

 **Mohamedk** 2 years, 11 months ago

Selected Answer: BD

[https://support.google.com/a/answer/7584076?hl=en&ref\\_topic=7563358](https://support.google.com/a/answer/7584076?hl=en&ref_topic=7563358)

upvoted 1 times

 **jcloud965** 3 years ago

Selected Answer: BD

B will allow to asses future external sharings

D will help to investigate past ones

upvoted 1 times

 **Kristuc** 3 years, 7 months ago

B+D is correct

upvoted 2 times

 **Twindaddy** 3 years, 8 months ago

It says E is one of the correct answers, but the question specifically states it DOESN'T want sharing blocked. I think it's B and D.


upvoted 1 times

 **TheZug** 3 years, 9 months ago

B and C, the Drive Audit Report can be set up to do alerts (<https://support.google.com/a/answer/9725685>) and the Aggregate Reports allow you to view total sharing.

The Activity dashboard is for users only. External sharing shouldn't be disabled, so E is incorrect.

upvoted 2 times

 **admcloud** 3 years, 10 months ago

Hello, what would be the correct answer?

upvoted 1 times

🗨️ 👤 **Solandy** 4 years ago

A and B

upvoted 3 times

🗨️ 👤 **saurabh1805** 4 years, 1 month ago

Question does ask external access to be blocked hence i would go with option B and D

upvoted 2 times

🗨️ 👤 **saurabh1805** 4 years, 1 month ago

not D, It should be C. aggregate report show both internal and external shared drive.

upvoted 3 times



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.

**Suggested Answer: D**

Community vote distribution

C (100%)

- 🗳️ 👤 **tahatabak** Highly Voted 4 years, 4 months ago  
 (C) <https://support.google.com/a/answer/167430?hl=en>  
 upvoted 10 times
- 🗳️ 👤 **nwk** Highly Voted 4 years, 5 months ago  
 (C) <https://support.google.com/a/answer/167430?hl=en#:~:text=Google%20Groups%20Collaborative%20Inboxes%20are,support%20or%20customer%20service%20teams>.  
 upvoted 5 times
- 🗳️ 👤 **MacBait** Most Recent 2 years, 5 months ago  
Selected Answer: C  
 C is correct. D doesn't make sense  
 upvoted 1 times
- 🗳️ 👤 **Kevin666** 2 years, 9 months ago  
 C is correct. <https://support.google.com/a/answer/167430?hl=en>  
 upvoted 1 times
- 🗳️ 👤 **jcloud965** 3 years ago  
Selected Answer: C  
 C is the best practice.  
 A will only spread the incoming mails to all members without any information of assignments or replies, B doesnt allow different access levels and D is wrong.  
 upvoted 5 times
- 🗳️ 👤 **Kristuc** 3 years, 7 months ago  
 C is correct  
 upvoted 2 times
- 🗳️ 👤 **admcloud** 3 years, 10 months ago  
 Answer C, would it be correct?  
 upvoted 1 times
- 🗳️ 👤 **Fadhli** 4 years ago  
 C. <https://support.google.com/a/answer/167430?hl=en>  
 upvoted 1 times
- 🗳️ 👤 **saaurabh1805** 4 years, 1 month ago  
 C is correct answer and best option here.  
 upvoted 3 times
- 🗳️ 👤 **saaurabh1805** 4 years, 1 month ago  
<https://support.google.com/a/answer/167430?hl=en>  
 upvoted 1 times

🗨️ 👤 **nwk** 4 years, 5 months ago

Should Be (B), question states User Account, and managed by multiple employees

<https://support.google.com/a/users/answer/170957?hl=en>

upvoted 5 times

🗨️ 👤 **Ntwizz** 4 years, 2 months ago

I think it is (C). It say various levels of access. With (B) delegates only have one level of access, which is Full access.

upvoted 4 times

Your employer, a media and entertainment company, wants to provision G Suite 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 G Suite 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.

**Suggested Answer:** B

Community vote distribution



D (88%) 13%

  **nwk** Highly Voted 4 years, 5 months ago

Should be (D)

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

upvoted 11 times



  **HateMicrosoft** Highly Voted 4 years, 3 months ago

The correct answer is D

<https://support.google.com/a/answer/1628009?hl=en>



Customize directories for teams or groups

upvoted 7 times

  **pradeepaR** Most Recent 2 years, 2 months ago

It should be D.

upvoted 1 times

  **MacBait** 2 years, 5 months ago

Selected Answer: D

It is D.

upvoted 1 times

  **Free09888** 2 years, 6 months ago

It is D

upvoted 1 times

  **ComputerGirl** 2 years, 7 months ago

The Answer is B. Would not make sense to create a separate director for the VIP's if it be hidden.

upvoted 1 times

  **Kevin666** 2 years, 9 months ago

Selected Answer: D

I think the correct answer is D

upvoted 1 times

  **Mr\_JJ** 2 years, 11 months ago

Selected Answer: B

<https://support.google.com/a/answer/7566446?hl=en> - Step 2: Organize your users

upvoted 1 times

  **Mr\_JJ** 2 years, 11 months ago

Selected Answer: D

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

upvoted 1 times

🗨️ 👤 **jcloud965** 3 years ago

**Selected Answer: D**

Users that are assigned a custom directory can find only people in that custom directory. They can find all shared external contacts. They can also find all Groups that are visible to them.

Users in organizational units that aren't assigned a custom directory can find either:

Everyone in the Directory, if their organizational unit doesn't inherit a custom directory, or

Only people in a custom directory, if their organizational unit inherits a custom directory from a parent organizational unit.

upvoted 4 times

🗨️ 👤 **Kristuc** 3 years, 7 months ago

B is correct

upvoted 1 times

🗨️ 👤 **cloudsecnovice** 3 years, 6 months ago

How did you conclude it was B?

upvoted 1 times

🗨️ 👤 **Kristuc** 3 years, 6 months ago

Sorry meant to go with D

upvoted 1 times

🗨️ 👤 **Andrea990211** 3 years, 9 months ago

D is the correct answer

upvoted 1 times

🗨️ 👤 **saarabh1805** 4 years, 1 month ago

D is correct answer here.

upvoted 4 times

🗨️ 👤 **Imz\_mhav** 4 years, 5 months ago

I think it should be A

upvoted 3 times

🗨️ 👤 **nwk** 4 years, 5 months ago

Vote for A

upvoted 4 times

🗨️ 👤 **Pakinter** 4 years, 2 months ago

If you turn directory sharing off, they wont be searchable neither for the senior employees, neither by themselves. So best approach is D.

upvoted 3 times

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 > G Suite > Gmail > Phishing Attempts
- C. Security > Dashboard > Spam Filter: Phishing
- D. Reporting > Reports > Phishing

**Suggested Answer: A**

Community vote distribution

C (100%)

🗳️ **nwk** Highly Voted 4 years, 5 months ago

Should be C

<https://support.google.com/a/answer/7492330?hl=en>

upvoted 13 times

🗳️ **HateMicrosoft** 4 years, 3 months ago

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

upvoted 2 times

🗳️ **Rickmx** Most Recent 2 years, 3 months ago

Selected Answer: C

C. It is a report that actually exists.

upvoted 1 times

🗳️ **Casper79** 2 years, 4 months ago

100% C

upvoted 1 times

🗳️ **MacBait** 2 years, 5 months ago

Selected Answer: C

A isn't even a thing. It's C.

upvoted 1 times

🗳️ **[Removed]** 2 years, 10 months ago

Selected Answer: C

correct answer is C

upvoted 1 times

🗳️ **[Removed]** 2 years, 10 months ago

Selected Answer: C

correct answer is C

upvoted 1 times

🗳️ **Mr\_JJ** 2 years, 11 months ago

C: Where would you find this information if the CISO asks? The most efficient way is using the Security Panel - ref:

<https://support.google.com/a/answer/7492330?hl=en>

upvoted 1 times

🗳️ **hsinghrhce** 3 years, 5 months ago

C is correct

upvoted 1 times

🗳️ **Kristuc** 3 years, 7 months ago


C is correct

upvoted 1 times

  **MoisesC** 4 years ago

Should be C definitely.

upvoted 1 times

  **saurabh1805** 4 years, 1 month ago

C is correct answer here.

upvoted 1 times

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 > G Suite > 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

**Suggested Answer: A**

Community vote distribution

A (100%)

🗨️ **Nico282** 11 months, 1 week ago

**Selected Answer: A**

Now is in Account > Account Settings > Preferences > Release preferences  
upvoted 1 times

🗨️ **[Removed]** 2 years, 10 months ago

**Selected Answer: A**

correct answer is A  
upvoted 1 times

🗨️ **yuchun** 3 years, 3 months ago

A is correct because schedule release give you more time to prepare  
upvoted 4 times

🗨️ **Kristuc** 3 years, 7 months ago

A is correct  
upvoted 1 times

🗨️ **cloudsecnovice** 3 years, 7 months ago

The closest thing to the answer is A. If you review the support article mentioned a few times. You will see that A makes the most sense.  
upvoted 1 times

🗨️ **admcloud** 3 years, 10 months ago

What would be the best answer, could you confirm?  
upvoted 1 times

🗨️ **brtest222** 3 years, 11 months ago

It is C  
<https://support.google.com/a/answer/172177?hl=en>  
upvoted 2 times

🗨️ **TestLab** 3 years, 12 months ago

A is correct.

<https://support.google.com/a/answer/172177?hl=en>

Scheduled Release track is the default option but can be changed to rapid released track by an admin.  
upvoted 3 times

🗨️ **saurabh1805** 4 years, 1 month ago

For me none of them seems to be correct answer. Closest answer is A.

<https://support.google.com/a/answer/172177?hl=en>

upvoted 2 times

 **nwk** 4 years, 5 months ago

<https://support.google.com/a/answer/172177?hl=en>

Rapid Release track—Your users are among the first to see new features when they're released to G Suite. This means your users typically can access new features immediately or soon after they're launched to consumers.

Scheduled Release track (default)—Your users get new features at least one week after they're released to Rapid Release domains. This gives you more time to prepare your organization for changes.

upvoted 3 times



Your company frequently hires from five to ten interns for short contract engagements and makes use of the same generically named G Suite accounts (e.g., user1@your-company.com, user2@your-company.com, user3@your-company.com). The manager of this program wants all email to these accounts routed to the manager's mailbox account also. What should you do?

- A. Setup address forwarding in each account's GMail setting menu.
- B. Set up recipient address mapping in GMail Advanced Settings.
- C. Configure an Inbound Gateway route.
- D. Give the manager delegated access to the mailboxes.

**Suggested Answer: C**

Reference:

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

Community vote distribution


B (90%) 10%

 **nwk** Highly Voted 4 years, 5 months ago

The manager of this program wants all email to these accounts routed to the manager's mailbox account also.

Routing option - it does not means mail routing/Default Routing, but just an optional setting with the Address Map itself

==> The questions requires email to be send to both intern and manager mailbox , so cannot use split delivery  
upvoted 7 times

 **Reda1974** Most Recent 1 year, 5 months ago

**Selected Answer: B**

I m wrong, it s B (tested)

Forget my 2 other comments

upvoted 2 times

 **Reda1974** 1 year, 5 months ago

**Selected Answer: C**

A et B are about Gmail setting and not Google admin. And you cannot trust user to make no changes on gmail settings.

With D, you lose history when you destriy mailbox.

So, C is for me the only possibility

upvoted 1 times

 **Reda1974** 1 year, 5 months ago

In B, they talk about Gmail and not Google Admin. You cannot trust users to not change a setting in gmail. So i think that i cannot be B.

upvoted 1 times

 **pradeepaR** 2 years, 2 months ago

It Should B. In the recipient mapping have to select "Also route to original destination". The reason being "The manager of this program wants all email to these accounts routed to the manager's mailbox account also."

upvoted 1 times

 **MacBait** 2 years, 5 months ago

It's B.


upvoted 1 times

 **Kevin666** 2 years, 9 months ago

**Selected Answer: B**

B is right answer

upvoted 1 times

 **nuts\_bee** 2 years, 11 months ago

**Selected Answer: B**

Redirect incoming messages with address maps

<https://support.google.com/a/answer/4524505>

upvoted 3 times

🗨️ 👤 **jcloud965** 3 years ago

**Selected Answer: B**

Mapping allows to also route to original destination. B is the correct answer.

upvoted 3 times

🗨️ 👤 **lily16** 3 years, 2 months ago

C should be correct. Option 'Also deliver to' in Routing rule gives option to deliver email to additional email address

upvoted 1 times

🗨️ 👤 **hsinghrhce** 3 years, 5 months ago

B is right answer

upvoted 1 times

🗨️ 👤 **Kristuc** 3 years, 7 months ago

B is correct

upvoted 1 times

🗨️ 👤 **MasterDarque** 3 years, 7 months ago

Which is the correct answer?

upvoted 2 times

🗨️ 👤 **admcloud** 3 years, 10 months ago

Option B, would be the best answer?

upvoted 1 times

🗨️ 👤 **TestLab** 3 years, 12 months ago

The correct answer is B. C is a trick answer. Nowhere in the questions shows the mail flow of the environment. So we can't safely use suggest C.

upvoted 1 times

🗨️ 👤 **saurabh1805** 4 years, 1 month ago

Clearly B seems to be Correct answer as per link <https://support.google.com/a/answer/4524505?hl=en>

upvoted 1 times

🗨️ 👤 **Pakinter** 4 years, 2 months ago

Clearly is B. For C you need a complete infrastructure including an inbound server a new MX record that will route all mail of your company not only the mail for affected users. Using a Mapping address you have the option to send the message to the original recipient as well as the new address and don't need mount an infrastructure for that.

upvoted 4 times

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.

**Suggested Answer: D**

Community vote distribution

D (100%)


 **TestLab** Highly Voted 3 years, 12 months ago

I believe the answer is C.

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

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

upvoted 12 times

 **tranduchuyhcm** Highly Voted 3 years, 6 months ago


D is correct

Because, the question mentioned 4 countries with 4 different languages.

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

We can choose OU, each OU will correspond to each sales office in each country. The footer will be translated into each country's language. It will then be added to the footer for each OU corresponding to that country

upvoted 10 times

 **2shyshy** Most Recent 1 year, 1 month ago

It appears to be that C is correct because there is no way to translate to other languages.

upvoted 1 times

 **RMO000** 2 years, 11 months ago

Selected Answer: D

It's 4 footers because It's 4 OUs

upvoted 3 times

 **jcloud965** 3 years ago

Selected Answer: D

Why should we ensure that each sales team is in their own OU if we don't need to have localized footer ?

C would have been something like "Ensure that each sales team is the same OU" to have only one footer.

upvoted 3 times

 **yuchun** 3 years, 3 months ago

I checked this <https://support.google.com/a/answer/2364576?hl=en>, and didn't find any way can have multi footer setting


~~

upvoted 2 times

 **Kristuc** 3 years, 7 months ago

C is correct

upvoted 4 times

 **admcloud** 3 years, 10 months ago

The best option is C?

upvoted 3 times

  **saurabh1805** 4 years, 1 month ago

Questions doest say anything about translation so I would go with option C.

upvoted 6 times

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

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

**Suggested Answer:** D

Reference:

<https://support.google.com/a/answer/9104586?hl=en>

*Community vote distribution*

D (100%)

- 🗨️ 👤 **saarabh1805** Highly Voted 👍 4 years, 1 month ago  
D is correct answer , as login is most targeted actions post phishing attack  
upvoted 5 times
- 🗨️ 👤 **[Removed]** Most Recent 🕒 2 years, 10 months ago  
Selected Answer: D  
correct answer is D  
upvoted 2 times
- 🗨️ 👤 **Kristuc** 3 years, 7 months ago  
D is correct  
upvoted 4 times
- 🗨️ 👤 **MikeFR** 3 years, 7 months ago  
the answer is D. <https://support.google.com/a/answer/6197480?hl=en>  
upvoted 3 times

A company using G Suite 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.

**Suggested Answer: D**

Reference:

<https://support.google.com/a/answer/175197?hl=en>


Community vote distribution

B (67%)


D (33%)

 **nwk** Highly Voted 4 years, 5 months ago


B is more secure isn't it?  
upvoted 9 times

 **Imz\_mhav** Highly Voted 4 years, 5 months ago

B. Security keys are the most secure form of 2SV and protect against phishing threats.  
<https://support.google.com/a/answer/175197?hl=en#keys&prompt&authentic&codes&phone&2sv&security>  
upvoted 6 times

 **cramo1207** Most Recent 2 years, 1 month ago

**Selected Answer: D**  
Like all are saying, 2FA with hardware keys is the recommended practice by google but i think that if you want protect to your organization inmediately you need enable the 2FA with the app is faster than wait to arrive the hardware keys, both answers are right, i'm just thinking in the faster option  
upvoted 2 times

 **MacBait** 2 years, 5 months ago

B is both the most secure solution and the one officially recommended by Google.  
upvoted 1 times

 **Kevin666** 2 years, 9 months ago

**Selected Answer: B**  
B is Google recommend practice.  
<https://support.google.com/a/answer/175197?hl=en#zippy=%2Cconsider-using-security-keys-in-your-business>  
upvoted 1 times

 **[Removed]** 2 years, 10 months ago

**Selected Answer: B**  
correct answer is B  
upvoted 1 times

 **jcloud965** 3 years ago

**Selected Answer: B**  
B is the most secure way  
upvoted 2 times

 **Mr\_JJ** 2 years, 11 months ago

It is the most secure way, but it is not the cheapest and users tend to lose them. D I believe is the correct answer  
upvoted 1 times

 **lily16** 3 years, 2 months ago

why not D ?  
upvoted 1 times

🗨️ 👤 **Kristuc** 3 years, 7 months ago

B is correct

upvoted 1 times

🗨️ 👤 **cloudsecnovice** 3 years, 7 months ago

B is the most secure way to enable 2SV or 2FA on a google identity. Please review the following support article for additional details.

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

upvoted 2 times

🗨️ 👤 **Andrea990211** 3 years, 9 months ago

B is the correct answer, is more secure

upvoted 3 times

🗨️ 👤 **ar18** 3 years, 10 months ago

yo admcloud, are u a bot? pls stop spamming all the questions. the discussion here clearly states that the answer is C. Hence the high number of upvotes to the above comments

upvoted 1 times

🗨️ 👤 **admcloud** 3 years, 10 months ago

the best option would be B?

upvoted 1 times

🗨️ 👤 **TestLab** 3 years, 12 months ago

B is Correct. Physical keys have always been stressed as the most secure method since the Advance Protection Program by Google themselves. <https://landing.google.com/advancedprotection/>

upvoted 2 times

🗨️ 👤 **saurabh1805** 4 years, 1 month ago

B for me as well

upvoted 3 times

🗨️ 👤 **Pakinter** 4 years, 2 months ago

B. Google recommends authenticator app only as an alternative to security keys in <https://support.google.com/a/answer/175197?hl=en> (Best practices for 2-Step Verification section)

upvoted 1 times

After migrating to G Suite, your legal team requests access to search all email and create litigation holds for employees who are involved with active litigation. You need to help the legal team meet this request. What should you do?

- A. Add the legal team to the User Management Admin system role.
- B. Add the legal team to the Google Vault Google Group.
- C. Create a custom role with Google Vault access, and add the legal team.
- D. Create a matter in Google Vault, and share with the legal team.

**Suggested Answer: C**

Reference:

<https://gsuite.google.com/products/vault/>

Community vote distribution

C (100%)

 **nwk** Highly Voted 4 years, 1 month ago

Vote for c


To open the shared matter, the account must be assigned an admin role with the Manage Holds, Manage Searches, Manage Exports, or Manage Audits privilege (or any combination). Learn more

upvoted 8 times

 **TestLab** Highly Voted 3 years, 12 months ago

C is correct. The legal team will need to control holds, search, and exports. They can't do that without having permission to do so.

upvoted 5 times

 **CyprienT** Most Recent 2 years, 6 months ago

Vote for C. The legal team needs to have a access via Google Vault

upvoted 1 times

 **jcloud965** 3 years ago

Selected Answer: C

C will give needed permission to access and use Vault


A will give too much permission and no Vault access. B is non sense. D doesn't allow legal team to do their own investigations later.

upvoted 1 times

 **Kristuc** 3 years, 7 months ago

C is correct

upvoted 1 times

 **Andrea990211** 3 years, 9 months ago

C is the correct answer. <https://support.google.com/vault/answer/2799699>

upvoted 2 times

 **admcloud** 3 years, 10 months ago


Could you confirm if option C would be the correct answer?

upvoted 1 times

 **saurabh1805** 4 years, 1 month ago

D is correct answer here.

upvoted 3 times

 **HateMicrosoft** 4 years, 3 months ago

D

<https://support.google.com/vault/answer/2462477>

upvoted 2 times

 **nwk** 4 years, 5 months ago

Even you share a matter, the user still need to be granted custom admin role to access the contents in Vault



upvoted 3 times

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.

**Suggested Answer:** D

Community vote distribution

D (100%)

 **nwk** Highly Voted 4 years, 5 months ago

Tricky about the clause - "any occurrence" of credit card numbers "and" your company's account number syntax, which is AccNo

Though reasonably should be either of the conditions matched, but question use "AND"

upvoted 6 times

 **MacBait** Most Recent 2 years, 5 months ago

Selected Answer: D

Only OUTBOUND (so cross both internal rules), then it also has to have BOTH AccNo AND CCNs, so it's D.

upvoted 1 times

 **jcloud965** 3 years ago

Selected Answer: D

Only OUTBOUND containing Credit Card Numbers AND AccNo

upvoted 1 times

 **Kristuc** 3 years, 7 months ago

D is correct

upvoted 1 times

 **TestLab** 3 years, 12 months ago

The answer is D.

It's a poorly written question. This should be an "either" condition since you want to catch any instances of Credit cards or AccNo being sent outside your domain.

upvoted 2 times

 **saarabh1805** 4 years, 1 month ago

D seems to be correct answer, Please refer below link.

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

upvoted 2 times

 **nwk** 4 years, 5 months ago

Only Advanced Content Match allow search using Regex (pattern) - So is D

upvoted 2 times

 **DickDastardly** 3 years, 8 months ago

This is the crucial factor which confirms D as the answer, despite the ambiguity of the question  
upvoted 1 times

Your company has decided to change SSO providers. Instead of authenticating into G Suite and other cloud services with an external SSO system, you will now be using Google as the Identity Provider (IDP) and SSO provider to your other third-party cloud services.

What two features are essential to reconfigure in G Suite? (Choose two.)

- A. Apps > add SAML apps to your domain.
- B. Reconfigure user provisioning via Google Cloud Directory Sync.
- C. Replace the third-party IDP verification certificate.
- D. Disable SSO with third party IDP.
- E. Enable API Permissions for Google Cloud Platform.

**Suggested Answer:** AC

Reference:

<https://support.google.com/a/answer/60224?hl=en>

Community vote distribution


AD (67%)

AC (33%)

 **nwk** Highly Voted 4 years, 5 months ago


Vote for A and D

upvoted 12 times

 **saurabh1805** Highly Voted 4 years, 1 month ago

A and D are correct answer here.

upvoted 9 times

 **cramo1207** Most Recent 2 years, 1 month ago

Selected Answer: AC

i think that the page answer is right because when you will use Google like IDP and SSO for the other cloud services, this ones need to configure url and certificates that generate in the admin.console when you are setting up this feature

upvoted 1 times

 **Dialex2006** 2 years, 3 months ago

Selected Answer: AD

Definitely A+D

upvoted 1 times

 **[Removed]** 2 years, 10 months ago

Selected Answer: AD

correct answer is A & D

upvoted 1 times

 **Kristuc** 3 years, 7 months ago

A+D is correct

upvoted 2 times

 **DanIRMark** 3 years, 9 months ago

is C not correct? changing providers would mean that a different certificate is needed.

upvoted 1 times

 **DanIRMark** 3 years, 9 months ago

Actually, 3rdP SSO would not need a certificate setup, so there is nothing to replace, so it cannot be C - So A and D is the most correct answer

upvoted 2 times

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

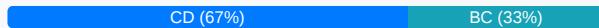
- A. Mac OS
- B. Windows
- C. Chrome OS
- D. iOS
- E. Linux

**Suggested Answer:** CD

Reference:

<https://support.google.com/a/answer/2634553?hl=en>

Community vote distribution



- 🗨️ **hsiaohan** 2 years, 7 months ago  
the correct answer is C and D, "mobile and Chrome OS devices"  
upvoted 1 times
- 🗨️ **hehe\_24** 2 years, 8 months ago  
yup, its c&d  
upvoted 1 times
- 🗨️ **Mgait** 2 years, 9 months ago  
**Selected Answer: BC**  
B/C/D? You can create a custom rule for windows management settings to Win devices that are managed.  
upvoted 1 times
- 🗨️ **[Removed]** 2 years, 10 months ago  
**Selected Answer: CD**  
correct answer is C & D  
upvoted 2 times
- 🗨️ **Kristuc** 3 years, 7 months ago  
C+D is correct  
upvoted 1 times
- 🗨️ **RHAdmin** 3 years, 7 months ago  
C and D >>>> <https://support.google.com/a/answer/2634553?hl=en>  
upvoted 1 times
- 🗨️ **admcloud** 3 years, 10 months ago  
What would be the correct answer?  
upvoted 1 times

Your-company.com recently bought 2500 Chrome devices and wants to distribute them to various teams globally. You decided that enterprise enrollment would be the best way to enforce company policies for managed Chrome devices. You discovered that Chrome devices currently end up in the top-level organization unit, and this needs to change to the organizational unit of the device administrator.

What should you do?

- A. Change Enrollment Permissions to only allow users in this organization to re-enroll existing devices.
- B. Change Enrollment Controls to Place Chrome device in user organization.
- C. Change Enrollment Controls to Keep Chrome device in current location.
- D. Change Enrollment Permissions to not allow users in this organization to enroll new devices.

**Suggested Answer: A**

Community vote distribution

B (100%)

🗳️ **Imz\_mhav** Highly Voted 4 years, 5 months ago

Vote for B.

[https://support.google.com/chrome/a/answer/2657289#auto\\_device\\_placement\\_enabled](https://support.google.com/chrome/a/answer/2657289#auto_device_placement_enabled)

Selecting Place Chrome device in user organization means that when you enroll the Chrome device, the device is placed in the organizational unit that the enrolling user is in. The settings you've applied for that user's organizational unit are applied to the device.

upvoted 10 times

🗳️ **HateMicrosoft** 4 years, 3 months ago

<https://support.google.com/chrome/a/answer/1360534?hl=en>

By default, devices automatically enroll in the top-level organizational unit. If you want devices to automatically enroll in the organizational unit that the user belongs to

upvoted 2 times

🗳️ **Mgait** Most Recent 2 years, 9 months ago

Selected Answer: B

B is correct.

upvoted 1 times

🗳️ **jcloud965** 3 years ago

Selected Answer: B

Selecting Place Chrome device in user organization means that when you enroll the Chrome device, the device is placed in the organizational unit that the enrolling user is in. The settings you've applied for that user's organizational unit are applied to the device.

upvoted 2 times

🗳️ **Kristuc** 3 years, 6 months ago

B is correct

upvoted 2 times

🗳️ **admcloud** 3 years, 10 months ago

The best option would be the answer B?

upvoted 1 times

🗳️ **saurabh1805** 4 years, 1 month ago

I also vote for B

upvoted 2 times

🗳️ **Pakinter** 4 years, 2 months ago

It is B. A is related to who can enroll devices not to what organization devices must be enrolled.

upvoted 2 times

  **leandrotorquato** 4 years, 4 months ago

I agree with the answer Imz\_mhav B is the right  
upvoted 3 times

A user has traveled overseas for an extended trip to meet with several vendors. The user has reported that important draft emails have not been saved in Gmail, which is affecting their productivity. They have been constantly moving between hotels, vendor offices, and airport lounges.

You have been tasked with troubleshooting the issue remotely. Your first priority is diagnosing and preventing this from happening again, and your second priority is recovering the drafts if possible. Due to time zone differences, and the user's busy meeting schedule, you have only been able to arrange a brief Hangouts Meet with the user to gather any required troubleshooting inputs. What two actions should be taken on this call with the user? (Choose two.)

- A. Ask the user to send an email to you so you can check the headers.
- B. Record a HAR file of the user composing a new email.
- C. Take screenshots of the user's screen when composing an email.
- D. Use the Email log search in the Admin panel.
- E. Check the Users > App Users Activity report.

**Suggested Answer:** CE

Community vote distribution

BC (100%)

🗨️ **saurobh1805** Highly Voted 4 years, 1 month ago  
b and D,

<https://support.google.com/a/answer/2604578?hl=en>  
upvoted 7 times

🗨️ **HateMicrosoft** Highly Voted 4 years, 3 months ago  
B&E  
Get the HAR file from the end user and check the user Apps usage.  
upvoted 5 times

🗨️ **jcloud965** Most Recent 3 years ago  
Selected Answer: BC

B. Record a HAR file of the user composing a new email will help diagnose any issue in the browser + C. Take screenshots of the user's screen when composing an email.

A. the headers are relevant only for sent or received emails ; D. Email log includes only sent or received emails ; E. Users > App Users Activity report will show (useless) information we can check before or after the call, like A and D  
upvoted 3 times

🗨️ **banface** 3 years ago

I agree with D since with User Reports: Apps usage you can find out if the user was using his Gmail with IMAP, POP or Web (since he was traveling around). POP3 downloads the email from a server to a single computer, then deletes the email from the server. On the other hand, IMAP stores the message on a server and synchronizes the message across multiple devices. So therefore, if using POP then the drafts would get deleted. Still unsure if screenshots or HAR file ... I think HAR file only works if you do it from your own browser, tricky question... any thoughts?  
upvoted 2 times

🗨️ **banface** 3 years ago

Record a HAR file of the user composing an email? That doesn't make sense to me, as it is the user who needs to record the HAR file from his Chrome browser to be analyzed. Also, how would email log search help to retrieve DRAFTS? Email log search is for SENT or RECEIVED emails... ??  
upvoted 1 times

🗨️ **Kristuc** 3 years, 6 months ago  
B+D is correct  
upvoted 4 times



🗨️ 👤 **DanIRMark** 3 years, 9 months ago

Tools available via the Google Admin Toolbox (<https://toolbox.googleapps.com/apps/main/>) would help. This is where you analyze the HAR file (making B correct) the toolbox also has a log analyzer making D correct

upvoted 2 times

🗨️ 👤 **admcloud** 3 years, 10 months ago

what would be the correct answer options? Thank you

upvoted 1 times

🗨️ 👤 **PCE\_Army** 3 years, 11 months ago

Why D ? we can do that after call.

upvoted 3 times

🗨️ 👤 **PCE\_Army** 3 years, 11 months ago

I would go C and E then.

upvoted 1 times

🗨️ 👤 **Fadhli** 4 years ago

B and D

upvoted 3 times

🗨️ 👤 **tahatabak** 4 years, 4 months ago

Why take screenshots of the user's screen when composing an email ?

upvoted 3 times

🗨️ 👤 **nwk** 4 years, 5 months ago

B & C ?

[https://toolbox.googleapps.com/apps/har\\_analyzer/](https://toolbox.googleapps.com/apps/har_analyzer/)

upvoted 3 times

Your company recently migrated to G Suite and wants to deploy a commonly used third-party app to all of finance. Your OU structure in G Suite is broken down by department. You need to ensure that the correct users get this app. What should you do?

- A. For the Finance OU, enable the third-party app in SAML apps.
- B. For the Finance OU, enable the third-party app in Marketplace Apps.
- C. At the root level, disable the third-party app. For the Finance OU, allow users to install any application from the G Suite Marketplace.
- D. At the root level, disable the third-party app. For the Finance OU, allow users to install only whitelisted apps from the G Suite Marketplace.



**Suggested Answer: B**

Reference:

<https://support.google.com/a/answer/6089179?hl=en>

Community vote distribution

 B (100%)

  **nwk** Highly Voted 4 years ago

(B) - Add to Domain List and choose only Finance OU



Tested we can't restrict "whitelisted app" per OU, whitelisted app is available domain-wide  
upvoted 7 times

  **DanIRMark** 3 years, 10 months ago

according to this link [<https://support.google.com/a/answer/172931?hl=en>] you CAN restrict whitelisted apps at a OU level, making D the correct answer  
upvoted 2 times

  **jadson88888** 3 years, 9 months ago

nwk was saying that we can't restrict "installing" whitelisted app per OU, and what mark gave is Turn on or off the service. vote for B  
upvoted 1 times

  **saurabh1805** Highly Voted 4 years, 1 month ago

I will go with Option B because D says just about marketplace apps and whitelisting but doesn't say if third party app will be enabled for them.,  
upvoted 5 times

  **jcloud965** Most Recent 3 years ago

**Selected Answer: B**  
You want to DEPLOY so you need to install it for the OU from Marketplace Apps.  
Whitelisting will allow users to use it but will not deploy it.  
upvoted 1 times

  **Kristuc** 3 years, 6 months ago

B is correct  
upvoted 1 times

  **Maxlee** 3 years, 9 months ago



B and E  
upvoted 1 times

  **admcloud** 3 years, 10 months ago

What would be the correct answer?  
upvoted 1 times

  **armada4wd** 4 years, 2 months ago

What about B? - doesn't say disable for other users and is a commonly used app  
upvoted 3 times

  **Ashfaq** 4 years, 3 months ago

I would go for D.  
upvoted 1 times

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

**Suggested Answer:** AC

Community vote distribution

AC (100%)

 **jcloud965** 3 years ago


**Selected Answer: AC**

A will help to determine why the message is considered as Spam.

and maybe C : it will prevent the sender to be considered as Spam again but it is not troubleshooting, it is solving the issue without knowing why it happens.

B will allow to access all the email content, not only the header but you are not a human spam detector. D. Email log search will only tell you "Spam detected", no more information than with A. E is useless since it is an inbound issue.

upvoted 4 times

 **mariusj** 3 years ago

The task is troubleshooting the issue, so you need to do actions in A and D. C is already a solution, and not an appropriate one since you can just add the sender to the Approved senders list.

upvoted 2 times

 **ashrafh** 3 years ago

I don't think "A" is the right option as I check my own spam email in this Google workspace Toolbox.

You can also check your own spam email and check from this link

<https://toolbox.googleapps.com/apps/messageheader/>

So my answer is

C and D

upvoted 1 times

 **HectorLeon2099** 3 years, 1 month ago

C+D is the best option

upvoted 1 times

 **Kristuc** 3 years, 6 months ago

A+C is correct

upvoted 1 times

 **admcloud** 3 years, 10 months ago


The best options would be A and C

upvoted 1 times

 **saarabh1805** 4 years, 1 month ago

I will also go with A and C here.

upvoted 4 times

 **Ntwizz** 4 years, 4 months ago

A and C is the correct answer.

upvoted 4 times

  **priatampan** 4 years, 4 months ago

i think the answer is B and C

upvoted 3 times

Security and Compliance has identified that data is being leaked through a third-party application connected to G Suite. You want to investigate using an audit log.

What log should you use?

- A. Admin audit log
- B. SAML audit log
- C. Drive usage audit log
- D. OAuth Token audit log

**Suggested Answer:** D

Reference:

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

*Community vote distribution*

D (100%)

🗨️ 👤 **[Removed]** 2 years, 10 months ago

**Selected Answer: D**

correct answer is D

upvoted 2 times

🗨️ 👤 **Kristuc** 3 years, 7 months ago

D is correct

upvoted 3 times

🗨️ 👤 **admcloud** 3 years, 10 months ago

Option D, would be the correct answer?

upvoted 1 times

🗨️ 👤 **saurabh1805** 4 years, 1 month ago

D is correct option here, A cant be because its just log console activity, B successful and failed sign-ins to SAML applications using the SAML audit log, C is just for drive.

upvoted 1 times

🗨️ 👤 **nwk** 4 years, 5 months ago

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

upvoted 4 times

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 G Suite. 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 G Suite.
- D. Configure USB Yubikeys for all users.

**Suggested Answer:** B

Community vote distribution

B (100%)

🗨️ **stiggypop** Highly Voted 4 years ago

Because they have blocked peripheral access to devices (a.k.a. they have disabled USB access so the device keys won't work) upvoted 5 times

🗨️ **jcloud965** Most Recent 3 years ago

Selected Answer: B

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. upvoted 3 times

🗨️ **Kristuc** 3 years, 7 months ago

B is correct upvoted 1 times

🗨️ **admcloud** 3 years, 10 months ago

Would the answer be option B? upvoted 1 times

🗨️ **Sorensen** 4 years ago

Can someone please explain how google authenticator is the correct answer? upvoted 2 times

🗨️ **TestLab** 3 years, 12 months ago

Even though Physical Keys are best practices, the option that is enabled on their environment does not allow them to use them. Blocked Peripheral access means no Yubikeys since USB ports are assumed disabled. upvoted 6 times

A company wants to distribute iOS devices to only the employees in the Sales OU. They want to be able to do the following on these devices:

- ⇒ Control password policies.
- ⇒ Make corporate apps available to the users.
- ⇒ Remotely wipe the device if it's lost or compromised

What two steps are required before configuring the device policies? (Choose two.)

- A. Turn on Advanced Mobile Management for the domain.
- B. Turn on Advanced Mobile Management for Sales OU
- C. Set up Device Approvals.
- D. Set up an Apple Push Certificate.
- E. Deploy Apple Certificate to every device.

**Suggested Answer:** AC

Community vote distribution

BD (100%)

🗳️ **nwk** Highly Voted 4 years, 5 months ago

B and D

<https://support.google.com/a/answer/7396025?hl=en>

<https://support.google.com/a/answer/6080359?hl=en>

upvoted 16 times

🗳️ **TestLab** Highly Voted 3 years, 12 months ago

It's B and D. You can't leverage the required features without configuring Apple Push Certification for iOS devices since these options are leveraging Advanced MDM. In addition, MDM Policies can be controlled at an OU level.

upvoted 6 times

🗳️ **Mgait** Most Recent 2 years, 9 months ago

Selected Answer: BD

B - Only sales OU is using IOS Devices.

D - Need Apple Certificate to utilize any of the MMD

upvoted 1 times

🗳️ **Mr\_JJ** 2 years, 11 months ago

Selected Answer: BD

B & D

<https://support.google.com/a/answer/7396025?hl=en>

upvoted 1 times

🗳️ **Kristuc** 3 years, 7 months ago

B+D is correct

upvoted 1 times

🗳️ **admcloud** 3 years, 10 months ago

B and D would be the most accurate answer options?

upvoted 1 times

🗳️ **saurabh1805** 4 years, 1 month ago

for me B and C is correct option.

Refer to below link to justify option C.

[https://support.google.com/a/answer/7508418?hl=en&ref\\_topic=1734198](https://support.google.com/a/answer/7508418?hl=en&ref_topic=1734198)

upvoted 2 times

🗳️ **saurabh1805** 4 years, 1 month ago

since this is company owned device C wotn be correct option, I will go with nwk option which is D



upvoted 1 times

Your client is a 5,000-employee company with a high turn-over rate that requires them to add and suspend user accounts. When new employees are onboarded, a user object is created in Active Directory. They have determined that manually creating the users in G Suite Admin Panel is time-consuming and prone to error.

You need to work with the client to identify a method of creating new users that will reduce time and error.


What should you do?

- A. Install Google Cloud Directory Sync on all Domain Controllers.
- B. Install G Suite Sync for Microsoft Outlook on all employees' computers.
- C. Install Google Cloud Directory Sync on a supported server.
- D. Install Google Apps Manager to automate add-user scripts.

**Suggested Answer: A**


Community vote distribution

C (100%)

 **Imz\_mhav** Highly Voted 4 years, 5 months ago


C - <https://support.google.com/a/answer/6123896>

upvoted 12 times

 **Pakinter** Highly Voted 4 years, 2 months ago

It is C. Google Cloud Sync Directory can is not needed in all the DC servers, just in one linux or windows supported server is enough. Depending of your directory size you can configure different GCDS servers for different synchronizations and split the workload, for example, one for profiels, another for contacts and another for groups.

upvoted 7 times

 **ESP\_SAP** Most Recent 2 years, 11 months ago

Correct Answer is (D):

Reduce time and errors.

Some Top GAM Use Cases

The command line allows simple operations to be done quickly without have to navigate the admin console for Workspace.

Create, update, delete, and view the following: users, groups, devices, OUs

gam info user [user@domain.com]

gam update user [user@domain.com] firstname [new firstname]

Bulk operations allow changes that would be tedious in the admin console. For example, update a group and synchronize it against multiple OUs (this command is all one line):

<https://www.ditoweb.com/2021/03/using-open-source-google-apps-manager-to-administer-google-workspace/>

upvoted 1 times

 **Toasty984** 2 years, 1 month ago

D is not correct, since GAM is NOT an official Google Product.

upvoted 1 times

 **jcloud965** 3 years ago

**Selected Answer: C**

GCDS server should only be able to access directory but shouldn't be installed on AD.

Better to install it on linux of course :)

GAM is a complicated option since we have GCDS available. A and B are wrong.

upvoted 1 times

 **Kristuc** 3 years, 7 months ago

C is correct

upvoted 1 times

🗨️ 👤 **Fadhli** 4 years ago

C is correct

upvoted 1 times

🗨️ 👤 **saurabh1805** 4 years, 1 month ago

I will got with GAM which is option D, GAM is amazing tools to automate user creation.

upvoted 3 times

🗨️ 👤 **certificationDJJ** 3 years, 1 month ago

it doesn't make sense

upvoted 1 times

🗨️ 👤 **aldrinzee** 3 years, 1 month ago

GAM is a third party and is for people with Deep Technical Knowledge

upvoted 1 times

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.

**Suggested Answer: A**

Reference:

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

Community vote distribution

A (100%)


 **saurabh1805** Highly Voted 4 years, 1 month ago

For me option A seems to be correct and closed to one.  
upvoted 6 times

 **jcloud965** Most Recent 3 years ago

Selected Answer: A

Randomly scattering auto-updates is an option built for this purpose : A.  
B & D Throttle the bandwidth or update over cellular are not acceptable solution in 2021. C Disable Auto update is not secured  
upvoted 3 times


 **justinp** 3 years, 6 months ago

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>

upvoted 2 times

 **Kristuc** 3 years, 6 months ago

A is correct  
upvoted 2 times

 **jadson88888** 3 years, 9 months ago

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

upvoted 2 times


Your company moved to G Suite 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.

**Suggested Answer:** D

Community vote distribution

A (100%)

 **saurabh1805** Highly Voted 4 years, 1 month ago


D seems to be correct answer here.  
upvoted 5 times

 **DanIRMark** 3 years, 10 months ago

I dont believe that D is correct, Live Stream is a type of meeting where there are few contributors but many viewers (like a keynote session), this is not the type of meeting the Q is asking for. C seems like the only option that allows you to join the right meeting without any action  
upvoted 2 times

 **DanIRMark** 3 years, 10 months ago

Actually, re-reading the last part of the question, this Q does focus on a training session scenario, which is like a keynote session, so D is correct.  
upvoted 3 times

 **jcloud965** Highly Voted 3 years ago

Selected Answer: A

As an admin you can remotely connect devices to a meeting with the meeting code or name.  
<https://support.google.com/meethardware/answer/6069329>  
upvoted 5 times


 **Mr\_JJ** Most Recent 2 years, 11 months ago

Selected Answer: A

begin receiving the training without having to take any actions to join the session. This can only be accomplished if the admin remotely starts the call. Streaming still needs for the user to press an option. Ref: <https://support.google.com/meethardware/answer/6069329>  
upvoted 3 times

 **banface** 3 years ago


D seems correct but as per this article: <https://support.google.com/meet/answer/9308630?hl=en&co=GENIE.Platform%3DDesktop> it says Note: Streaming does not automatically start. During the meeting, at the bottom right, click Live Streaming and then Start streaming.  
upvoted 1 times

 **Kristuc** 3 years, 6 months ago

D is correct  
upvoted 2 times


 **juliog101** 3 years, 7 months ago

A? [https://support.google.com/meethardware/answer/6069329?hl=en&ref\\_topic=3341450](https://support.google.com/meethardware/answer/6069329?hl=en&ref_topic=3341450)  
upvoted 4 times

 **JLT** 3 years, 10 months ago

B is the correct answer (Not D, you can't auto-join a meeting)

upvoted 2 times

  **admcloud** 3 years, 10 months ago

D is the correct option?

upvoted 2 times

  **Fadhli** 4 years ago

D is correct

upvoted 3 times

  **Yei** 4 years, 3 months ago

A is correct

upvoted 3 times

  **nwk** 4 years, 5 months ago

<https://support.google.com/meet/answer/9308630?co=GENIE.Platform%3DDesktop&hl=en&oco=0>

upvoted 1 times

Your corporate LDAP contains the email addresses of several hundred non-employee business partners. You want to sync these contacts to G Suite so they appear in Gmail's address autocomplete for all users in the domain.

What are two options to meet this requirement? (Choose two.)

- A. Use the Directory API to upload a .csv file containing the contacts.
- B. Configure GCDS to populate a Group with external members.
- C. Use the People API to upload a .csv file containing the contacts.
- D. Develop a custom application to call the Domain Shared Contacts API.
- E. Configure GCDS to synchronize shared contacts.

**Suggested Answer: AD**

Community vote distribution

DE (67%)

AE (33%)



  **nwk** Highly Voted 4 years, 5 months ago

D and E

<https://support.google.com/a/answer/9281635?hl=en>

<https://support.google.com/a/answer/6162412#contacts>

upvoted 11 times

  **pradeepaR** Most Recent 2 years, 2 months ago

D and E

They want to sync non employee contact- which requires Domain Shared Contact API

Or they can sync using GCDS as shared contacts

upvoted 2 times

  **breakkanny** 2 years ago

Hey pradeep I just want to know do this certificate still valid cuz Google changed into Google workspace . If so can I take this question as preparation into Google workspace

upvoted 1 times

  **Kevin666** 2 years, 9 months ago

Selected Answer: DE

I choose D and E.

[https://support.google.com/a/answer/9281635?hl=en&ref\\_topic=20016](https://support.google.com/a/answer/9281635?hl=en&ref_topic=20016)

upvoted 1 times

  **Kevin666** 2 years, 9 months ago

Selected Answer: AE

I choose A and E.

[https://support.google.com/a/answer/9935004?hl=en&ref\\_topic=20016](https://support.google.com/a/answer/9935004?hl=en&ref_topic=20016)



upvoted 1 times

  **[Removed]** 2 years, 10 months ago

Selected Answer: DE


correct answer is D & E

upvoted 1 times

  **Kristuc** 3 years, 6 months ago

D+E is correct

upvoted 1 times

  **admcloud** 3 years, 10 months ago

D and E would be the correct answers?

upvoted 1 times

  **Fadhli** 4 years ago

D and E is correct



upvoted 1 times

  **saurabh1805** 4 years, 1 month ago

I will go with option A and E, as that's what google recommends to use. Refer below link for more information. Two options which are recommended by google are Directory API and GCDS attribute.

[https://support.google.com/a/answer/9935004?hl=en&ref\\_topic=20016](https://support.google.com/a/answer/9935004?hl=en&ref_topic=20016)

upvoted 4 times

  **holahola** 3 years, 10 months ago

A is wrong because you need to use Domain Shared Contacts API and not the Directory API for shared contacts. So the answer still is D and E.

upvoted 1 times

  **DanIRMark** 3 years, 10 months ago

The Shared Contacts API is used to manage contacts, not the Directory API. The Directory API can update employee details as detailed here : <https://developers.google.com/admin-sdk/directory?hl=en> so A cannot be correct

upvoted 1 times

  **priatampan** 4 years, 4 months ago

agree D and E

upvoted 1 times



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.

**Suggested Answer:** DE

Community vote distribution

BC (100%)

 **nwk** Highly Voted 4 years, 5 months ago

B and C also can

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


Use holds to preserve data indefinitely to meet legal or preservation obligations.

upvoted 17 times

 **nwk** Highly Voted 4 years, 5 months ago

A and B


upvoted 5 times

 **[Removed]** Most Recent 2 years, 10 months ago

Selected Answer: BC

correct answer is B & C


upvoted 2 times

 **jcloud965** 3 years ago

Selected Answer: BC


You have to create a new matter in Google Vault with a hold on the user's mailbox in Google Vault to override the default preservation rule.

upvoted 2 times

 **Kristuc** 3 years, 6 months ago

B+C is correct

upvoted 1 times

 **admcloud** 3 years, 10 months ago

Hello, what would be the correct answers?


upvoted 1 times

 **vamos** 3 years, 10 months ago

A and B.

I think that C can not be possible because the retention rule always apply to UO.

upvoted 1 times

 **1ewj7** 3 years, 11 months ago

D can not be possible because the user would know. So B and C.

upvoted 1 times

 **Fadhli** 4 years ago

B and C is correct

upvoted 1 times

  **saurabh1805** 4 years, 1 month ago

B and C is correct answer here.

upvoted 1 times

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 G Suite 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.

**Suggested Answer: D**

Reference:

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

Community vote distribution

D (100%)

🗨️ **frenzer** 2 years, 4 months ago

**Selected Answer: D**

D is correct. Downloading the user information from AC > Users will show the user status for all users and their OU.

C is incorrect since it will show in the report only the changes of user status in the last 6 months so the data might be incomplete.  
upvoted 1 times

🗨️ **jcloud965** 3 years ago

**Selected Answer: D**

D : you can get as a Google Sheet the list of all users including OUs and User state (active or suspended), and all other information like Storage used, last sign in, ....But should be "All columns" and not "Currently selected columns".

upvoted 2 times

🗨️ **Kristuc** 3 years, 6 months ago

C is correct

upvoted 1 times

🗨️ **Andrea990211** 3 years, 9 months ago

D is the correct answer.

upvoted 2 times

🗨️ **Andrea990211** 3 years, 9 months ago

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

upvoted 1 times

🗨️ **Andrea990211** 3 years, 9 months ago

Sorry, error ... you have to go into user reports to see the status of each user and then export the content to a google sheet, so the right answer is C ---><https://support.google.com/cloudidentity/answer/4580176?hl=en#zippy=%2Cgeneral>

upvoted 3 times

🗨️ **truclink** 3 years, 1 month ago

If you export data to Google Sheet from Aggregate reports, you cannot view suspended user accounts by Org unit, you can selected Manager Reports, there is no information about suspended user accounts

upvoted 1 times

🗨️ **admcloud** 3 years, 10 months ago

option D confirmed?

upvoted 1 times

🗨️ 👤 **vamos** 3 years, 10 months ago

Vote D

upvoted 1 times

🗨️ 👤 **saurabh1805** 4 years, 1 month ago

D is also correct option for me,

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

upvoted 4 times

🗨️ 👤 **saurabh1805** 4 years, 1 month ago

Sorry it should be C, as aggregate will show the numbers of users as asked in questions.

upvoted 6 times

You recently started an engagement with an organization that is also using G Suite. 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.

**Suggested Answer: A**

Community vote distribution

D (100%)

🗨️ 👤 **pradeepaR** 2 years, 2 months ago

Option A: Without turning on External sharing, how we can share the file with team drive.

upvoted 1 times

🗨️ 👤 **rodriguessilva** 2 years, 11 months ago

**Selected Answer: D**

Option A is a partial solution, it does not prevent internal sharing.

upvoted 3 times

🗨️ 👤 **jcloud965** 3 years ago

**Selected Answer: D**

D will centralize information in a secured area where only approved, internal and external users can collaborate.

upvoted 2 times

🗨️ 👤 **Mr\_JJ** 2 years, 11 months ago

Yeah but if you have Frontline, G Suite basic or Workspace Business Starter, they won't be able to only view the shared drive content within their organization. So it will be a limited access.

upvoted 1 times

🗨️ 👤 **Kristuc** 3 years, 6 months ago

D is correct

upvoted 2 times

🗨️ 👤 **DanIRMark** 3 years, 10 months ago

Option A is a partial solution, it does not prevent internal sharing. Option D is the correct option

upvoted 1 times

🗨️ 👤 **nwk** 4 years, 1 month ago

go for D

upvoted 2 times

🗨️ 👤 **saurabh1805** 4 years, 1 month ago

I will also go with Option D

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

upvoted 1 times

🗨️ 👤 **JoseLeandro** 4 years, 3 months ago

A allows to share with the whitelisting domain but not protect for been sharing with others, D allows to collaborate and limits the sharing


upvoted 2 times

🗨️ 👤 **leandrotorquato** 4 years, 3 months ago

correct answer letter D

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

upvoted 1 times

  **lmz\_mhav** 4 years, 5 months ago

D

Based from the question, the data needs to be protected from being shared with unauthorized parties both internally and externally.

upvoted 3 times

You have configured your G Suite account on the scheduled release track to provide additional time to prepare for new product releases and determine how they will impact your users. There are some new features on the latest roadmap that your director needs you to test as soon as they become generally available without changing the release track for the entire organization. What should you do?

- A. Create a new OU and turn on the rapid release track just for this OU.
- B. Create a new Google Group with test users and enable the rapid release track.
- C. Establish a separate Dev environment, and set it to rapid release.
- D. Ask Google for a demo account with beta access to the new features.

**Suggested Answer: A**

Reference:

<https://support.google.com/a/answer/172177?hl=en>

Community vote distribution

C (100%)

- 🗨️ **saurobh1805** Highly Voted 4 years, 1 month ago  
C is best possible option, this is only way you can achieve this.  
upvoted 11 times
- 🗨️ **lily16** 3 years, 2 months ago  
This setting cannot be applied at OU level. So C is correct.  
upvoted 4 times
- 🗨️ **holahola** 3 years, 10 months ago  
Agree on this, because question also mentions "as soon as it is generally available". So we do not need beta features but rather rapid release track on Demo environment. If question would be written differently i would choose D then, but not in this case.  
upvoted 2 times
- 🗨️ **nwk** Highly Voted 4 years, 5 months ago  
Vote for C. Admin console cannot set rapid/schedule release by OU  
upvoted 6 times
- 🗨️ **DanIRMark** 3 years, 10 months ago  
This seems like the correct option, but find it hard to believe that Google does not provide this setting at a OU level.  
upvoted 1 times
- 🗨️ **1209apl** Most Recent 2 years, 3 months ago  
Selected Answer: C  
Answer is "C". There is no OU setting.  
upvoted 1 times
- 🗨️ **breakkanny** 2 years ago  
Hey mate . I want to know Google changed this certificate into Google workspace so can I take this exam as preparation into Google workspace exam  
upvoted 1 times
- 🗨️ **lcn** 2 years ago  
Collaboration Engineer has been renamed to Workspace Admin, it is the same exam.  
upvoted 1 times
- 🗨️ **ESP\_SAP** 2 years, 11 months ago  
Correct answer is (C):

Tip for large organizations: Select the Scheduled Release track for your production account. Then set up Rapid Release on a test account to try new features before they're available to your users.

<https://support.google.com/a/answer/172177>

upvoted 1 times

🗨️ 👤 **jcloud965** 3 years ago

**Selected Answer: C**

A dev account is the best way because you can't define this setting on a OU or group basis.

upvoted 2 times

🗨️ 👤 **Acloudeng** 3 years, 3 months ago

I think it is B because as shown in the Google article in the following link:

<https://support.google.com/a/answer/172177?hl=en>

Tip for large organizations: Select the Scheduled Release track for your production account. Then set up Rapid Release on a test account to try new features before they're available to your users.

upvoted 1 times

🗨️ 👤 **justinp** 3 years, 6 months ago

Isn't possible activate a rapid release to one OU, just entire Admin Console. I vote D.

upvoted 2 times

🗨️ 👤 **Kristuc** 3 years, 6 months ago

A is correct

upvoted 1 times

🗨️ 👤 **RHAdmin** 3 years, 7 months ago

The correct answer is C as explained on this page --> <https://support.google.com/a/answer/172177>

upvoted 1 times

🗨️ 👤 **admcloud** 3 years, 10 months ago

option C confirmed?

upvoted 2 times

🗨️ 👤 **dxxc** 4 years, 1 month ago

It's D

because it's Available G Suite Beta Programs to try newest product offerings

<https://www.cloudconnectcommunity.com/ccg/g-suite/g-suite-early-adopter-programs>

upvoted 1 times

🗨️ 👤 **Happy2b** 4 years, 5 months ago

@nwk : How to create separate Dev environment ? You mean to say get separate G Suite Demo account from Google ?

upvoted 2 times