

 Google Discussions

Exam Professional Cloud Security Engineer All Questions

View all questions & answers for the Professional Cloud Security Engineer exam

[Go to Exam](#)

EXAM PROFESSIONAL CLOUD SECURITY ENGINEER TOPIC 1 QUESTION 97 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 97

Topic #: 1

[\[All Professional Cloud Security Engineer Questions\]](#)

Your organization has implemented synchronization and SAML federation between Cloud Identity and Microsoft Active Directory. You want to reduce the risk of Google Cloud user accounts being compromised. What should you do?

- A. Create a Cloud Identity password policy with strong password settings, and configure 2-Step Verification with security keys in the Google Admin console.
- B. Create a Cloud Identity password policy with strong password settings, and configure 2-Step Verification with verification codes via text or phone call in the Google Admin console.
- C. Create an Active Directory domain password policy with strong password settings, and configure post-SSO (single sign-on) 2-Step Verification with security keys in the Google Admin console.
- D. Create an Active Directory domain password policy with strong password settings, and configure post-SSO (single sign-on) 2-Step Verification with verification codes via text or phone call in the Google Admin console.

[Show Suggested Answer](#)

by  [mouchu](#) at May 17, 2022, 9:41 a.m.

Comments

Type your comment...

[Submit](#)

  **coco10k** Highly Voted  1 year, 9 months ago

Answer C:



"We recommend against using text messages. The National Institute of Standards and Technology (NIST) no longer recommends SMS-based 2SV due to the hijacking risk from state-sponsored entities."

   upvoted 6 times

  **gcpengineer** 1 year, 2 months ago

user account doesnt need admin console access

   upvoted 1 times

  **uiuiui** Most Recent  8 months, 3 weeks ago

Selected Answer: C

"C" Please

   upvoted 2 times

  **AwesomeGCP** 1 year, 9 months ago

Selected Answer: C

C. Create an Active Directory domain password policy with strong password settings, and configure post-SSO (single sign-on) 2-Step Verification with security keys in the Google Admin console.

   upvoted 3 times

  **jitu028** 1 year, 9 months ago

Answer is - C

https://cloud.google.com/identity/solutions/enforce-mfa#use_security_keys

Use security keys

We recommend requiring security keys for those employees who create and access data that needs the highest level of security. You should require 2SV for all other employees and encourage them to use security keys.

Security keys offer the most secure form of 2SV. They are based on the open standard developed by Google as part of the Fast Identity Online (FIDO) Alliance. Security keys require a compatible browser on user devices.

   upvoted 2 times

  **AzureDP900** 1 year, 8 months ago

Agree with C and explanation

   upvoted 1 times

  **szl0144** 2 years, 2 months ago

C is the answer because security key is securer than 2FA code

   upvoted 4 times

  **mT3** 2 years, 2 months ago

Selected Answer: C

C is correct answer

   upvoted 4 times

  **mouchu** 2 years, 2 months ago

Answer = B

   upvoted 1 times



[Platform](#)

> [Home](#)

> [Examtopics PRO](#)

> [All Exams](#)

> [Training Courses](#)

