Course 4_Lab 2: Explore false positives through incident detection

Scenario

Your team lead, Chloe, has been notified of a low severity security alert. The alert identified a service account with broad permissions using insecure key management practices through user managed keys. Upon further investigation it was found that Hank, the cloud architect, unintentionally triggered this alert. Hank was testing a new service account and accidentally created the key for the test user account. This alert was addressed and closed as a false positive.

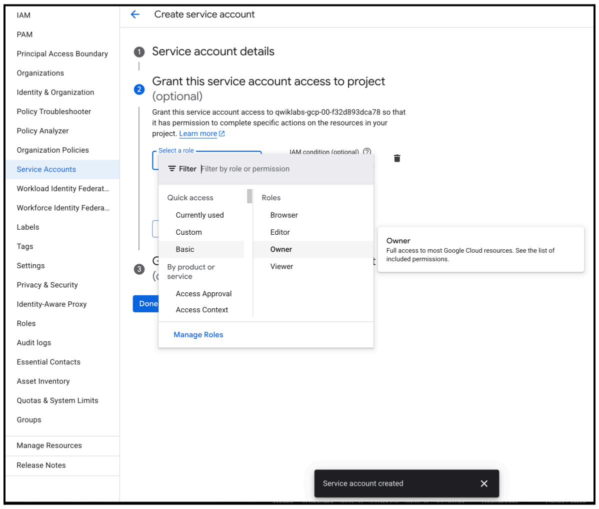
Chloe believes this alert serves as a great example of a false positive alert. Chloe has tasked you with recreating the activity that triggered the false positive alert. You'll analyze the alert and then remediate it. The process of recreating the false positive serves as a valuable learning experience that will help you understand how and why the alert was triggered and how you can implement effective security policies to mitigate further false positive alerts.

Here's how you'll do this task: **First**, you'll recreate the false positive by creating a service account, assigning a role, providing a key, and activating the service account. **Then**, you'll use Security Command Center (SCC) to access the vulnerability finding related to activity you triggered. **Finally**, you'll take action to remediate the vulnerability finding and take action to remediate the false positive.

MY WORK:

Task 1: Create a service account

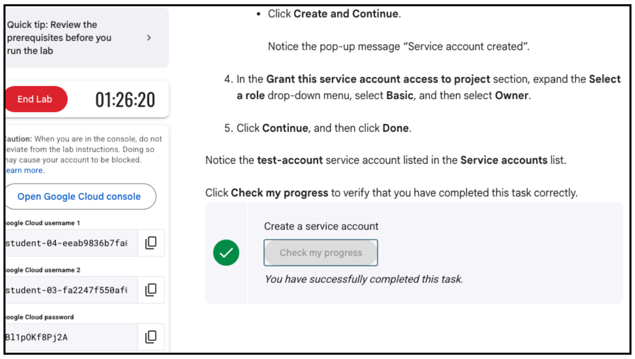
In this task, I created a service account and granted a role to use as a test account.



Grant this service account access to qwiklabs-gcp-00-f32d893dca78 so that it has permission to complete specific actions on the resources in your project. Learn more

Owner
Full access to most Google Cloud resources. See the list of included permissions.

Service account created


Quick tip: Review the prerequisites before you run the lab
End Lab
01:26:20
Open Google Cloud console
Check my progress

aution: When you are in the console, do not eviate from the lab instructions. Doing so nay cause your account to be blocked. earn more.

oogle Cloud username 1
student-04-eeab9836b7fa(

oogle Cloud username 2
student-03-fa2247f550af(

oogle Cloud password
B11pOKf8Pj2A

- Click **Create and Continue**.

  Notice the pop-up message "Service account created".

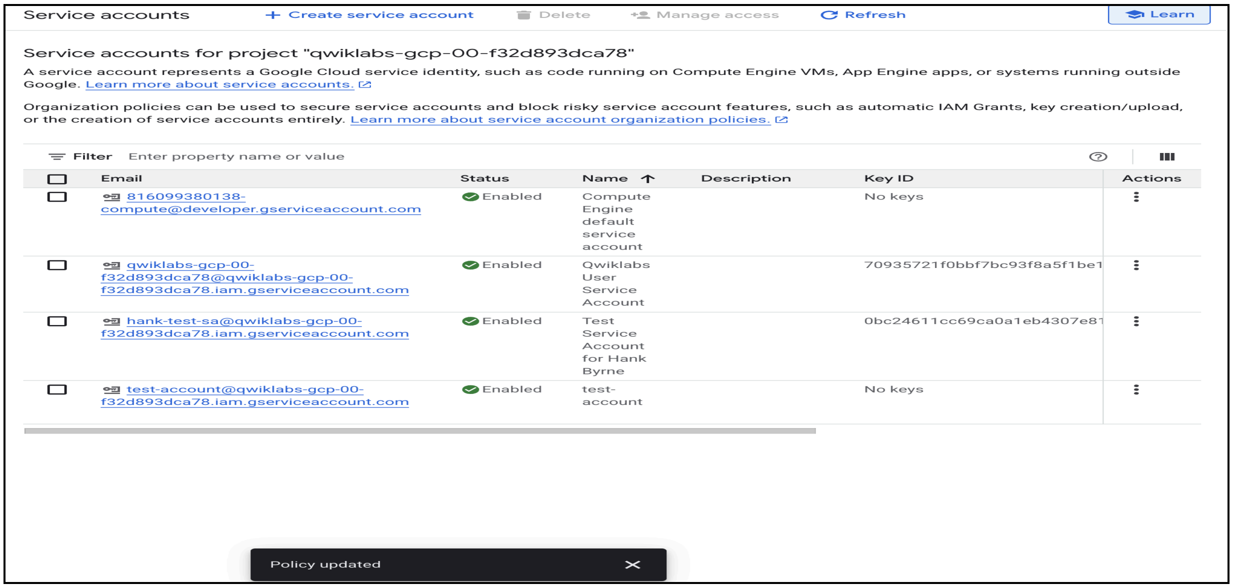
4. In the **Grant this service account access to project** section, expand the **Select a role** drop-down menu, select **Basic**, and then select **Owner**.
5. Click **Continue**, and then click **Done**.

Notice the **test-account** service account listed in the **Service accounts** list.

Click **Check my progress** to verify that you have completed this task correctly.

Create a service account

You have successfully completed this task.



Service accounts for project "qwiklabs-gcp-00-f32d893dca78"

A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or systems running outside Google. Learn more about service accounts.

Organization policies can be used to secure service accounts and block risky service account features, such as automatic IAM Grants, key creation/upload, or the creation of service accounts entirely. Learn more about service account organization policies.

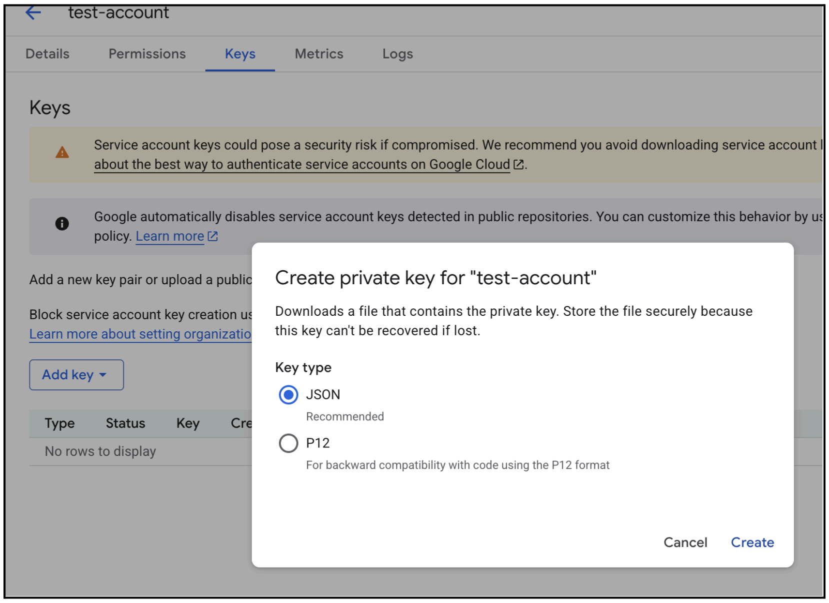
Filter Enter property name or value

□	Email	Status	Name ↑	Description	Key ID	Actions
□	816099380138-compute@developer.gserviceaccount.com	✓ Enabled	Compute Engine default service account		No keys	⋮
□	qwiklabs-gcp-00-f32d893dca78@qwiklabs-gcp-00-f32d893dca78.iam.gserviceaccount.com	✓ Enabled	Qwiklabs User Service Account		70935721f0bbf7bc93f8a5f1be1	⋮
□	hank-test-sa@qwiklabs-gcp-00-f32d893dca78.iam.gserviceaccount.com	✓ Enabled	Test Service Account for Hank Byrne		0bc24611cc69ca0a1eb4307e81	⋮
□	test-account@qwiklabs-gcp-00-f32d893dca78.iam.gserviceaccount.com	✓ Enabled	test-account		No keys	⋮

Policy updated ✕

Task 2: Create a JSON authentication key for your service account

In this task I created a JSON key and uploaded the file via Cloud Shell.



Keys

Service account keys could pose a security risk if compromised. We recommend you avoid downloading service account l
about the best way to authenticate service accounts on Google Cloud.

Google automatically disables service account keys detected in public repositories. You can customize this behavior by us
policy. Learn more

Add a new key pair or upload a public

Block service account key creation us
Learn more about setting organizatio

Type	Status	Key	Cre
No rows to display			

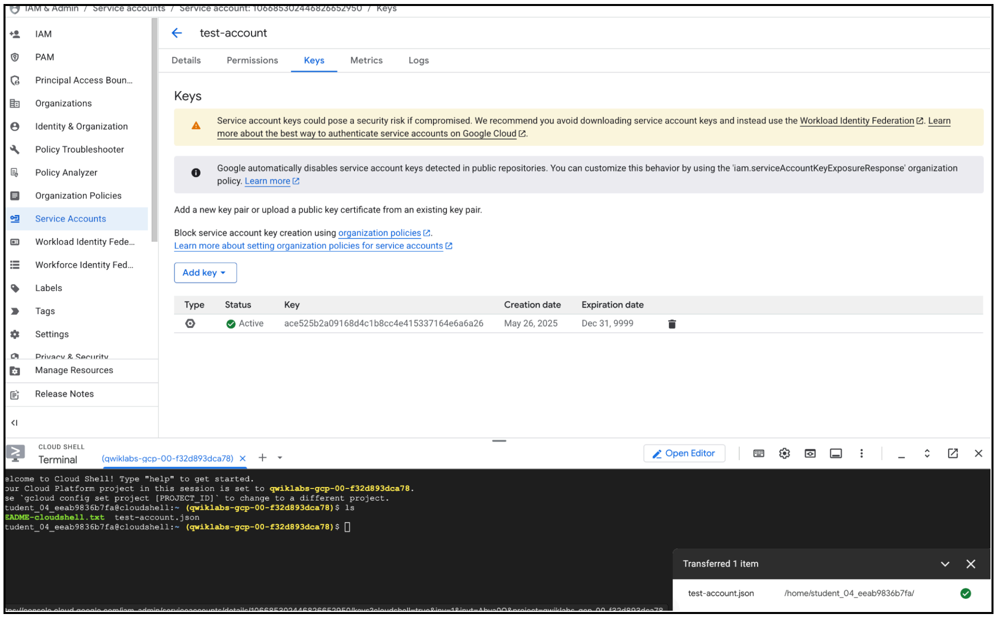
Create private key for "test-account"

Downloads a file that contains the private key. Store the file securely because this key can't be recovered if lost.

Key type

● JSON
Recommended

○ P12
For backward compatibility with code using the P12 format



test-account

Keys

Service account keys could pose a security risk if compromised. We recommend you avoid downloading service account keys and instead use the Workload Identity Federation. Learn more about the best way to authenticate service accounts on Google Cloud.

Google automatically disables service account keys detected in public repositories. You can customize this behavior by using the 'iam.serviceAccountKeyExposureResponse' organization policy. Learn more

Add a new key pair or upload a public key certificate from an existing key pair.

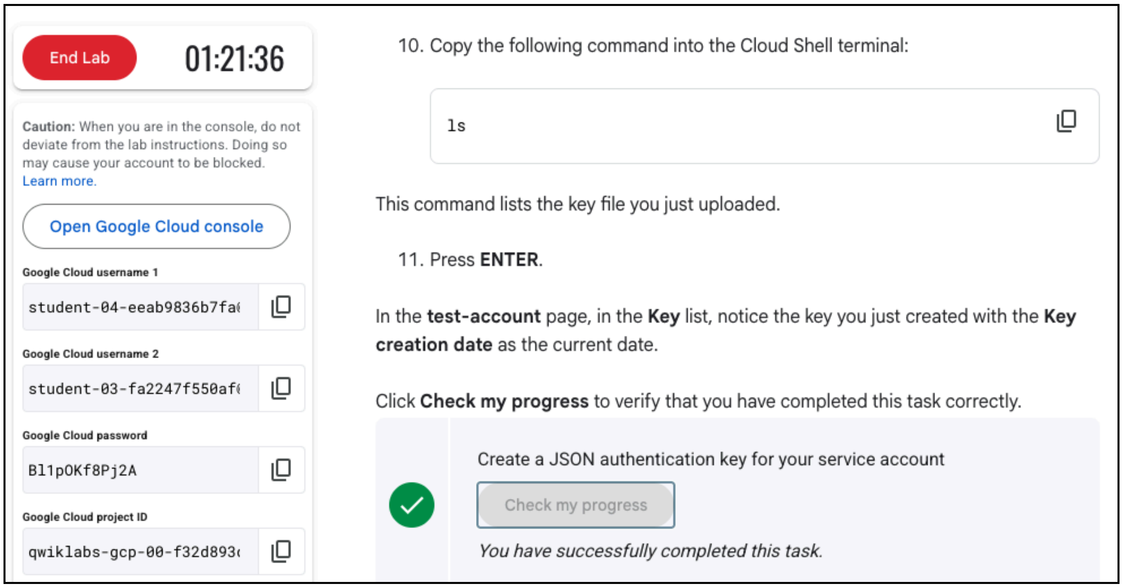
Block service account key creation using organization policies.
Learn more about setting organization policies for service accounts

Type	Status	Key	Creation date	Expiration date
⚙	✓ Active	ace525b2a09168d4c1b8cc4e415337164e6a6a26	May 26, 2025	Dec 31, 9999

```
elcome to Cloud Shell! Type "help" to get started.
our Cloud Platform project in this session is set to qwiklabs-gcp-00-f32d893dca78.
se `gcloud config set project [PROJECT_ID]` to change to a different project.
tudent_04_eeab9836b7fa@cloudshell:~ (qwiklabs-gcp-00-f32d893dca78)$ ls
EADME-cloudshell.txt  test-account.json
tudent_04_eeab9836b7fa@cloudshell:~ (qwiklabs-gcp-00-f32d893dca78)$ 
```

Transferred 1 item

test-account.json /home/student_04_eeab9836b7fa/ ✓



Caution: When you are in the console, do not deviate from the lab instructions. Doing so may cause your account to be blocked. Learn more.

Google Cloud username 1

student-04-eeab9836b7fa(

Google Cloud username 2

student-03-fa2247f550af(

Google Cloud password

Bl1pOKf8Pj2A

Google Cloud project ID

qwiklabs-gcp-00-f32d893(

10. Copy the following command into the Cloud Shell terminal:

```
ls
```

This command lists the key file you just uploaded.

11. Press **ENTER**.

In the **test-account** page, in the **Key** list, notice the key you just created with the **Key creation date** as the current date.

Click **Check my progress** to verify that you have completed this task correctly.

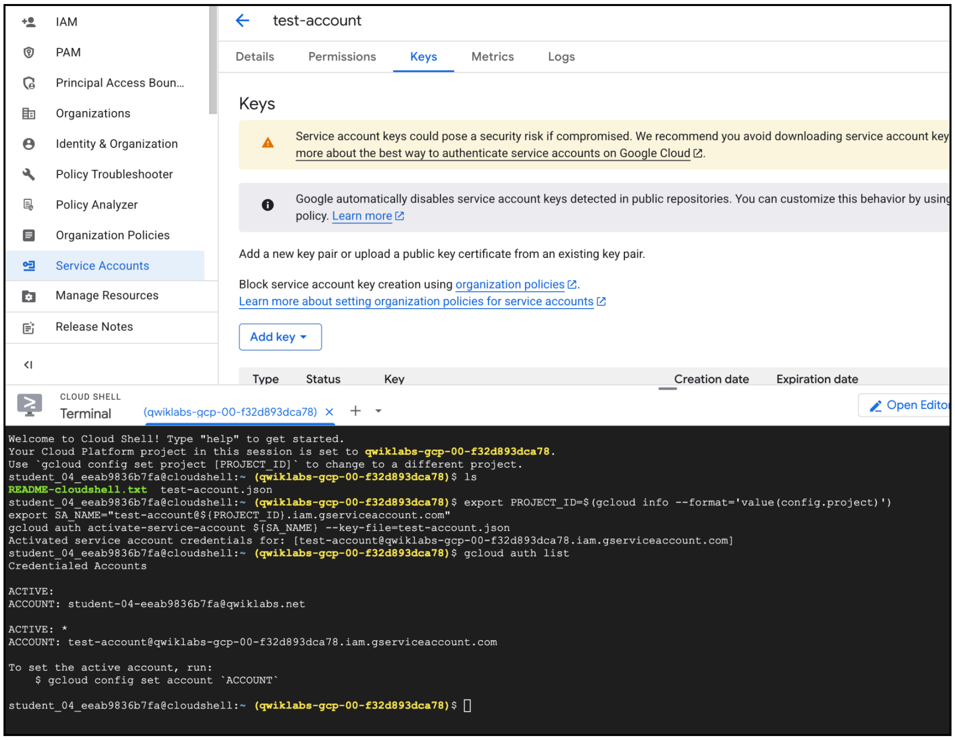
✓ Create a JSON authentication key for your service account

Check my progress

You have successfully completed this task.

Task 3: Trigger the false positive finding

In this task I added a command, provided by Google, to Cloud Shell to activate the service test account created in Task 1. In addition, I added another command that grants an additional role and permission to the user account to trigger a threat detection.



Keys

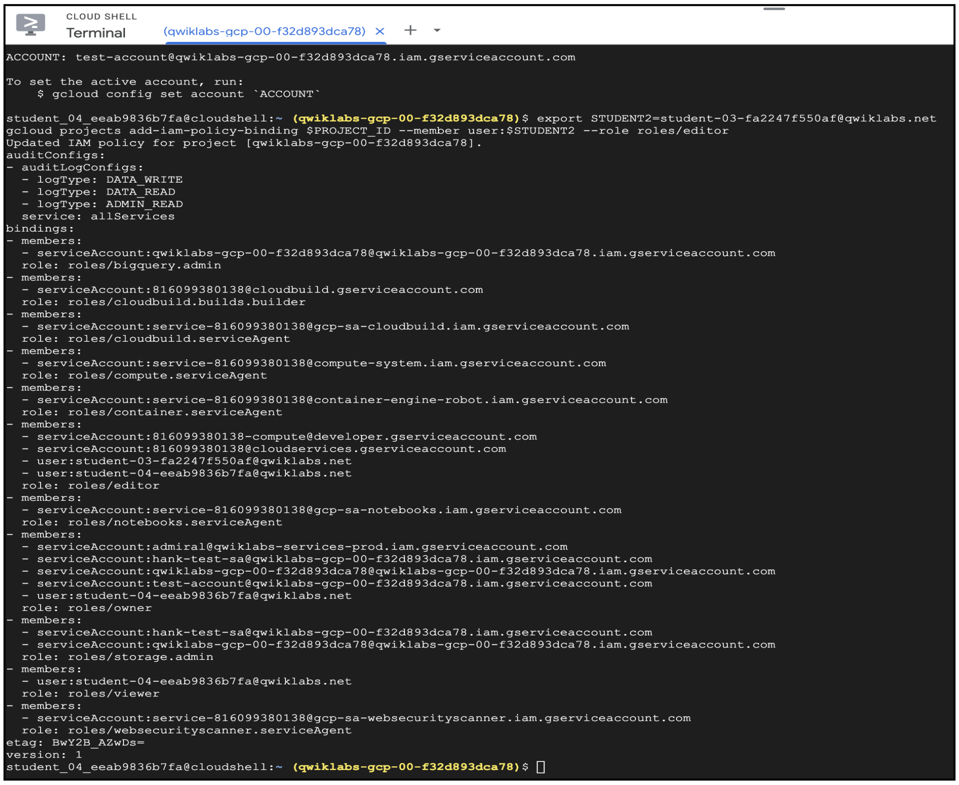
Service account keys could pose a security risk if compromised. We recommend you avoid downloading service account key
more about the best way to authenticate service accounts on Google Cloud.

Google automatically disables service account keys detected in public repositories. You can customize this behavior by using
policy. Learn more

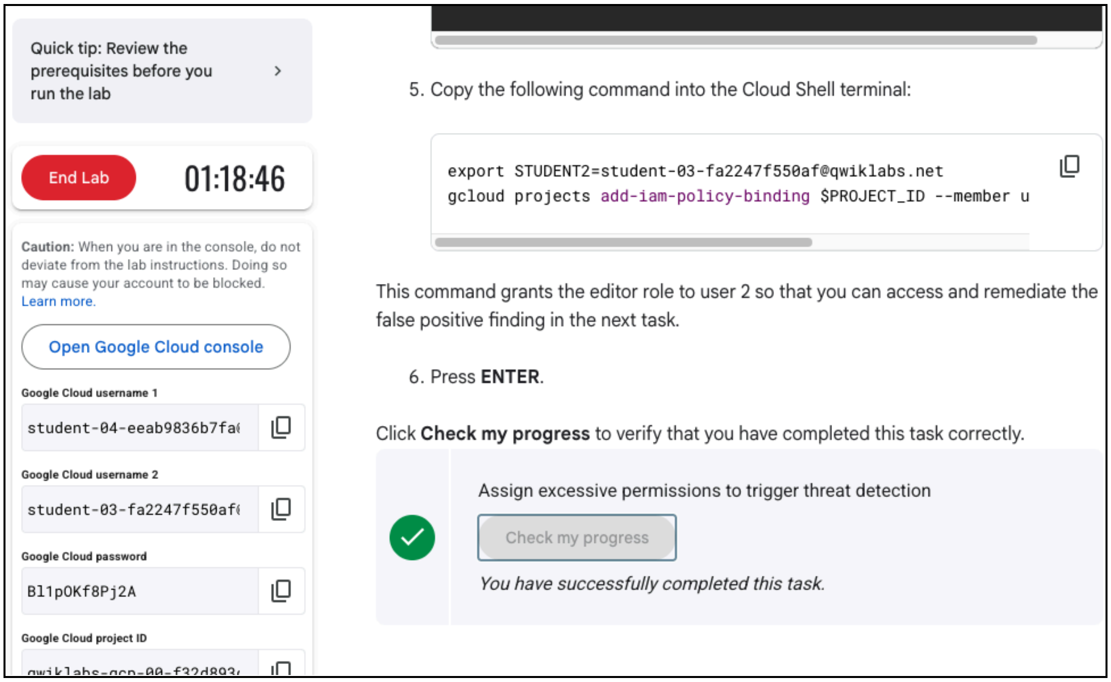
Add a new key pair or upload a public key certificate from an existing key pair.

Block service account key creation using organization policies.
Learn more about setting organization policies for service accounts

```
Welcome to Cloud Shell! Type "help" to get started.
Your Cloud Platform project in this session is set to qwiklabs-gcp-00-f32d893dca78.
Use `gcloud config set project [PROJECT_ID]` to change to a different project.
student_04_eeab9836b7fa@cloudshell:~ (qwiklabs-gcp-00-f32d893dca78)$ ls
README-cloudshell.txt  test-account.json
student_04_eeab9836b7fa@cloudshell:~ (qwiklabs-gcp-00-f32d893dca78)$ export PROJECT_ID=$(gcloud info --format='value(config.project)')
export SA_NAME="test-account@${PROJECT_ID}.iam.gserviceaccount.com"
gcloud auth activate-service-account ${SA_NAME} --key-file=test-account.json
Activated service account credentials for: [test-account@qwiklabs-gcp-00-f32d893dca78.iam.gserviceaccount.com]
student_04_eeab9836b7fa@cloudshell:~ (qwiklabs-gcp-00-f32d893dca78)$ gcloud auth list
Credentialed Accounts

ACTIVE:
ACCOUNT: student-04-eeab9836b7fa@qwiklabs.net

ACTIVE: *
ACCOUNT: test-account@qwiklabs-gcp-00-f32d893dca78.iam.gserviceaccount.com

To set the active account, run:
    $ gcloud config set account `ACCOUNT`

student_04_eeab9836b7fa@cloudshell:~ (qwiklabs-gcp-00-f32d893dca78)$ 
```



```
ACCOUNT: test-account@qwiklabs-gcp-00-f32d893dca78.iam.gserviceaccount.com

To set the active account, run:
    $ gcloud config set account `ACCOUNT`

student_04_eeab9836b7fa@cloudshell:~ (qwiklabs-gcp-00-f32d893dca78)$ export STUDENT2=student-03-fa2247f550af@qwiklabs.net
gcloud projects add-iam-policy-binding $PROJECT_ID --member user:$STUDENT2 --role roles/editor
Updated IAM policy for project [qwiklabs-gcp-00-f32d893dca78].
auditConfigs:
- auditLogConfigs:
  - logType: DATA_WRITE
  - logType: DATA_READ
  - logType: ADMIN_READ
  service: allServices
bindings:
- members:
  - serviceAccount:qwiklabs-gcp-00-f32d893dca78@qwiklabs-gcp-00-f32d893dca78.iam.gserviceaccount.com
  role: roles/bigquery.admin
- members:
  - serviceAccount:816099380138@cloudbuild.gserviceaccount.com
  role: roles/cloudbuild.builds.builder
- members:
  - serviceAccount:service-816099380138@gcp-sa-cloudbuild.iam.gserviceaccount.com
  role: roles/cloudbuild.serviceAgent
- members:
  - serviceAccount:service-816099380138@compute-system.iam.gserviceaccount.com
  role: roles/compute.serviceAgent
- members:
  - serviceAccount:service-816099380138@container-engine-robot.iam.gserviceaccount.com
  role: roles/container.serviceAgent
- members:
  - serviceAccount:816099380138-compute@developer.gserviceaccount.com
  - serviceAccount:816099380138@cloudservices.gserviceaccount.com
  - user:student-03-fa2247f550af@qwiklabs.net
  - user:student-04-eeab9836b7fa@qwiklabs.net
  role: roles/editor
- members:
  - serviceAccount:service-816099380138@gcp-sa-notebooks.iam.gserviceaccount.com
  role: roles/notebooks.serviceAgent
- members:
  - serviceAccount:admiral@qwiklabs-services-prod.iam.gserviceaccount.com
  - serviceAccount:hank-test-sa@qwiklabs-gcp-00-f32d893dca78.iam.gserviceaccount.com
  - serviceAccount:qwiklabs-gcp-00-f32d893dca78@qwiklabs-gcp-00-f32d893dca78.iam.gserviceaccount.com
  - serviceAccount:test-account@qwiklabs-gcp-00-f32d893dca78.iam.gserviceaccount.com
  - user:student-04-eeab9836b7fa@qwiklabs.net
  role: roles/owner
- members:
  - serviceAccount:hank-test-sa@qwiklabs-gcp-00-f32d893dca78.iam.gserviceaccount.com
  - serviceAccount:qwiklabs-gcp-00-f32d893dca78@qwiklabs-gcp-00-f32d893dca78.iam.gserviceaccount.com
  role: roles/storage.admin
- members:
  - user:student-04-eeab9836b7fa@qwiklabs.net
  role: roles/viewer
- members:
  - serviceAccount:service-816099380138@gcp-sa-websecurityscanner.iam.gserviceaccount.com
  role: roles/websecurityscanner.serviceAgent
etag: BwY2B_AZwDs=
version: 1
student_04_eeab9836b7fa@cloudshell:~ (qwiklabs-gcp-00-f32d893dca78)$ 
```



Quick tip: Review the prerequisites before you run the lab

01:18:46

Caution: When you are in the console, do not deviate from the lab instructions. Doing so may cause your account to be blocked. Learn more.

Google Cloud username 1

student-04-eeab9836b7fa

Google Cloud username 2

student-03-fa2247f550af

Google Cloud password

Bl1pOKf8Pj2A

Google Cloud project ID

qwiklabs-gcp-00-f32d893

5. Copy the following command into the Cloud Shell terminal:

```
export STUDENT2=student-03-fa2247f550af@qwiklabs.net
gcloud projects add-iam-policy-binding $PROJECT_ID --member u
```

This command grants the editor role to user 2 so that you can access and remediate the false positive finding in the next task.

6. Press **ENTER**.

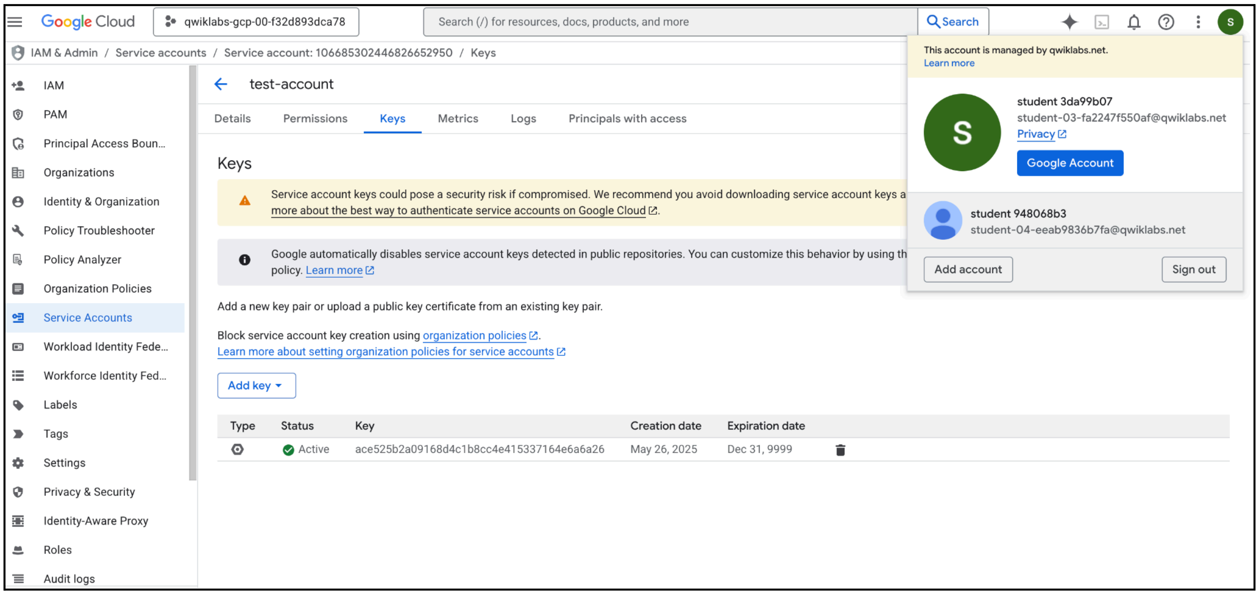
Click **Check my progress** to verify that you have completed this task correctly.

Assign excessive permissions to trigger threat detection

You have successfully completed this task.

Task 4: Sign in as the second user

In this task, I only needed to sign in to the user test account.



Google Cloud
qwiklabs-gcp-00-f32d893dca78
Search (/) for resources, docs, products, and more
Search
S

IAM & Admin / Service accounts / Service account: 106685302446826652950 / Keys

test-account

Keys

Service account keys could pose a security risk if compromised. We recommend you avoid downloading service account keys a
more about the best way to authenticate service accounts on Google Cloud.

Google automatically disables service account keys detected in public repositories. You can customize this behavior by using th
policy. Learn more

Add a new key pair or upload a public key certificate from an existing key pair.

Block service account key creation using organization policies.
Learn more about setting organization policies for service accounts

Type	Status	Key	Creation date	Expiration date
⚙	✓ Active	ace525b2a09168d4c1b8cc4e415337164e6a6a26	May 26, 2025	Dec 31, 9999

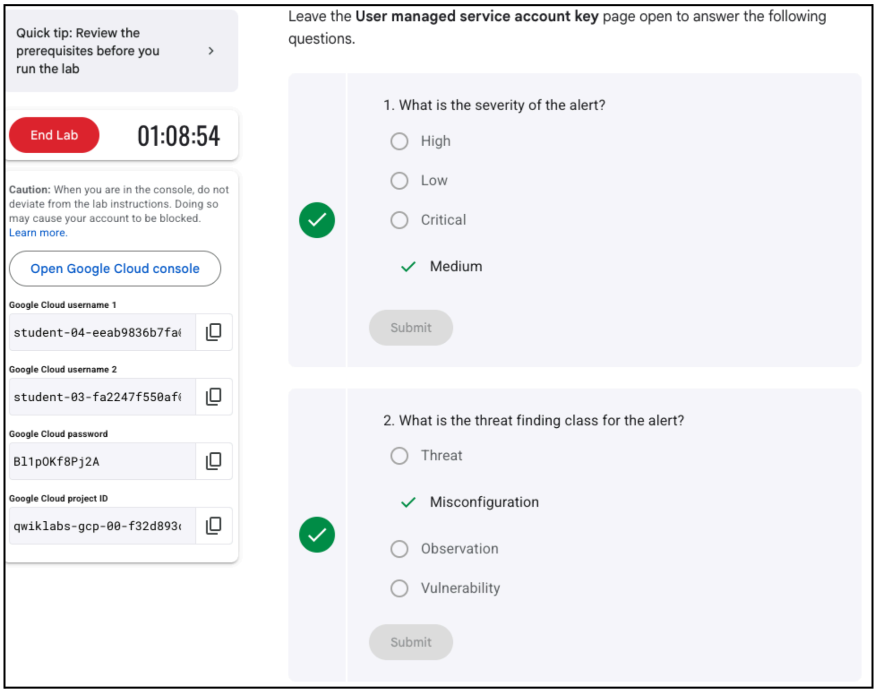
This account is managed by qwiklabs.net.
Learn more

student 3da99b07
student-03-fa2247f550af@qwiklabs.net
Privacy

student 948068b3
student-04-eeab9836b7fa@qwiklabs.net

Task 5: View the threat finding in SCC

In this task, I reviewed the findings in the Security Command Center (SCC) and answered a series of questions about the severity level and the threat class.



Quick tip: Review the prerequisites before you run the lab ›

End Lab 01:08:54

Caution: When you are in the console, do not deviate from the lab instructions. Doing so may cause your account to be blocked. Learn more.

Open Google Cloud console

Google Cloud username 1: student-04-eeab9836b7fa(

Google Cloud username 2: student-03-fa2247f550af(

Google Cloud password: Bl1pOKf8Pj2A

Google Cloud project ID: qwiklabs-gcp-00-f32d893(

Leave the **User managed service account key** page open to answer the following questions.

1. What is the severity of the alert?

○ High

○ Low

○ Critical

✓ Medium

Submit

2. What is the threat finding class for the alert?

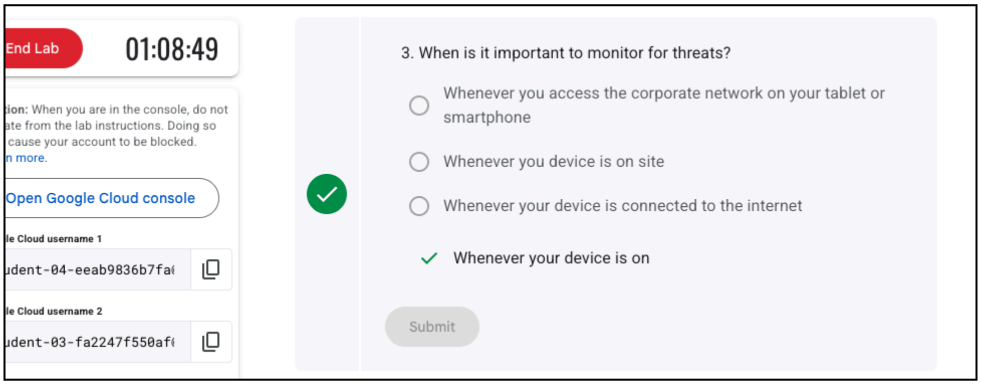
○ Threat

✓ Misconfiguration

○ Observation

○ Vulnerability

Submit



End Lab 01:08:49

ion: When you are in the console, do not ate from the lab instructions. Doing so cause your account to be blocked. n more.

Open Google Cloud console

le Cloud username 1: udent-04-eeab9836b7fa(

le Cloud username 2: udent-03-fa2247f550af(

3. When is it important to monitor for threats?

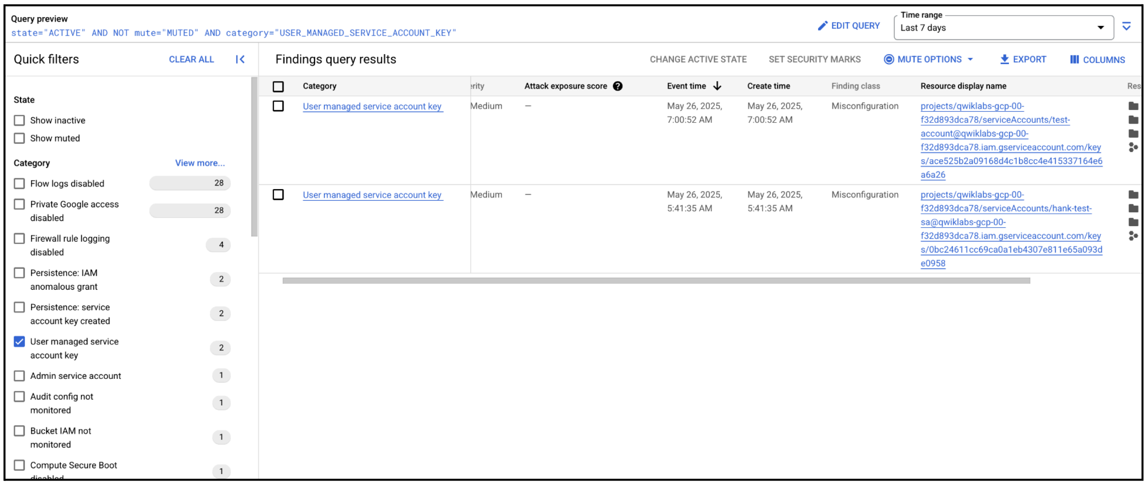
○ Whenever you access the corporate network on your tablet or smartphone

○ Whenever you device is on site

○ Whenever your device is connected to the internet

✓ Whenever your device is on

Submit



Query preview

```
state="ACTIVE" AND NOT mute="MUTED" AND category="USER_MANAGED_SERVICE_ACCOUNT_KEY"
```

EDIT QUERY

Time range: Last 7 days

Quick filters CLEAR ALL

State

□ Show inactive

□ Show muted

Category View more...

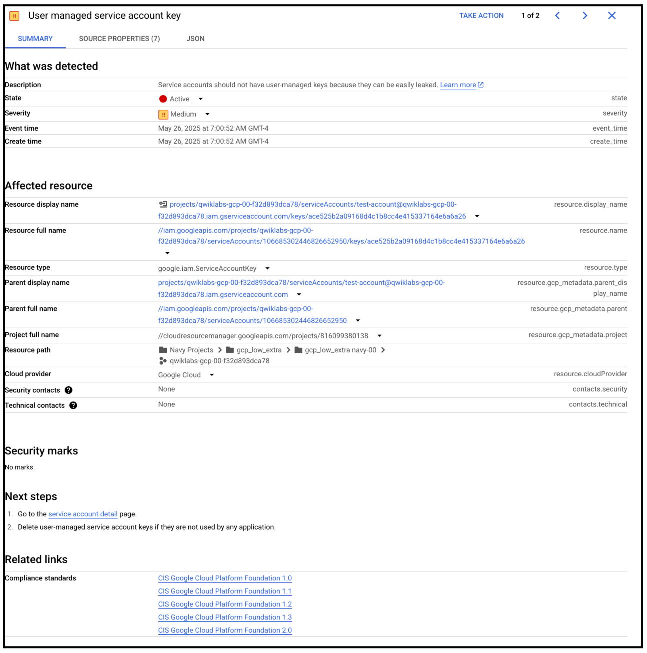
□ Flow logs disabled	28
□ Private Google access disabled	28
□ Firewall rule logging disabled	4
□ Persistence: IAM anomalous grant	2
□ Persistence: service account key created	2
☑ User managed service account key	2
□ Admin service account	1
□ Audit config not monitored	1
□ Bucket IAM not monitored	1
□ Compute Secure Boot disabled	1

Findings query results

CHANGE ACTIVE STATE SET SECURITY MARKS MUTE OPTIONS EXPORT COLUMNS

□	Category	rity	Attack exposure score	Event time	Create time	Finding class	Resource display name
□	User managed service account key	Medium	–	May 26, 2025, 7:00:52 AM	May 26, 2025, 7:00:52 AM	Misconfiguration	projects/qwiklabs-gcp-00-f32d893dca78/serviceAccounts/test-account@qwiklabs-gcp-00-f32d893dca78.iam.gserviceaccount.com/keys/ace525b2a09168d4c1b8cc4e415337164e6a6a26
□	User managed service account key	Medium	–	May 26, 2025, 5:41:35 AM	May 26, 2025, 5:41:35 AM	Misconfiguration	projects/qwiklabs-gcp-00-f32d893dca78/serviceAccounts/hank-test-sa@qwiklabs-gcp-00-f32d893dca78.iam.gserviceaccount.com/keys/0bc24611cc69ca0a1eb4307e811e65a093de0958

In this specific step of the task, the Google answer indicated that the information was found under Summary, however, explanation of the threat, and recommendation on how to handle the threat were not listed under that section. However, all three were listed under the Source Properties tab.



What was detected

Description	Service accounts should not have user-managed keys because they can be easily leaked. Learn more	
State	● Active	state
Severity	Medium	severity
Event time	May 26, 2025 at 7:00:52 AM GMT-4	event_time
Create time	May 26, 2025 at 7:00:52 AM GMT-4	create_time

Affected resource

Resource display name	projects/qwiklabs-gcp-00-f32d893dca78/serviceAccounts/test-account@qwiklabs-gcp-00-f32d893dca78.iam.gserviceaccount.com/keys/ace525b2a09168d4c1b8cc4e415337164e6a6a26	resource.display_name
Resource full name	//iam.googleapis.com/projects/qwiklabs-gcp-00-f32d893dca78/serviceAccounts/106685302446826652950/keys/ace525b2a09168d4c1b8cc4e415337164e6a6a26	resource.name
Resource type	google.iam.ServiceAccountKey	resource.type
Parent display name	projects/qwiklabs-gcp-00-f32d893dca78/serviceAccounts/test-account@qwiklabs-gcp-00-f32d893dca78.iam.gserviceaccount.com	resource.gcp_metadata.parent_display_name
Parent full name	//iam.googleapis.com/projects/qwiklabs-gcp-00-f32d893dca78/serviceAccounts/106685302446826652950	resource.gcp_metadata.parent
Project full name	//cloudresourcemanager.googleapis.com/projects/816099380138	resource.gcp_metadata.project
Resource path	Navy Projects > gcp_low_extra > gcp_low_extra navy-00 > qwiklabs-gcp-00-f32d893dca78	
Cloud provider	Google Cloud	resource.cloudProvider
Security contacts	None	contacts.security
Technical contacts	None	contacts.technical

Security marks

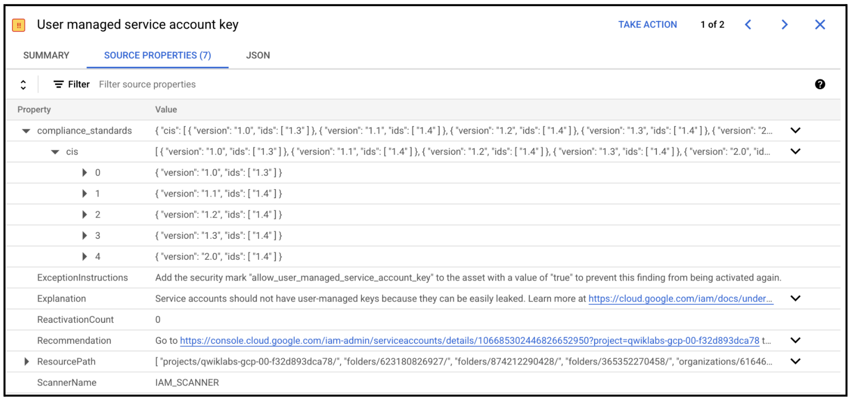
No marks

Next steps

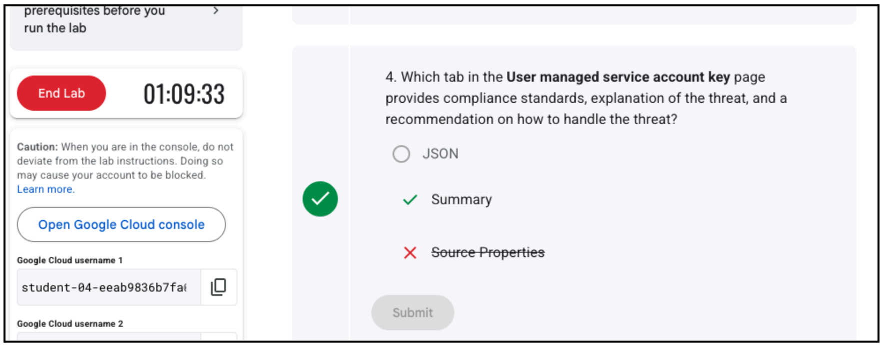
1. Go to the service account detail page.
2. Delete user-managed service account keys if they are not used by any application.

Related links

Compliance standards	CIS Google Cloud Platform Foundation 1.0 CIS Google Cloud Platform Foundation 1.1 CIS Google Cloud Platform Foundation 1.2 CIS Google Cloud Platform Foundation 1.3 CIS Google Cloud Platform Foundation 2.0



Property	Value
compliance_standards	{ "cis": [{ "version": "1.0", "ids": ["1.3"] }, { "version": "1.1", "ids": ["1.4"] }, { "version": "1.2", "ids": ["1.4"] }, { "version": "1.3", "ids": ["1.4"] }, { "version": "2...
cis	[{ "version": "1.0", "ids": ["1.3"] }, { "version": "1.1", "ids": ["1.4"] }, { "version": "1.2", "ids": ["1.4"] }, { "version": "1.3", "ids": ["1.4"] }, { "version": "2.0", "id...
0	{ "version": "1.0", "ids": ["1.3"] }
1	{ "version": "1.1", "ids": ["1.4"] }
2	{ "version": "1.2", "ids": ["1.4"] }
3	{ "version": "1.3", "ids": ["1.4"] }
4	{ "version": "2.0", "ids": ["1.4"] }
ExceptionInstructions	Add the security mark "allow_user_managed_service_account_key" to the asset with a value of "true" to prevent this finding from being activated again.
Explanation	Service accounts should not have user-managed keys because they can be easily leaked. Learn more at https://cloud.google.com/iam/docs/under...
ReactivationCount	0
Recommendation	Go to https://console.cloud.google.com/iam-admin/serviceaccounts/details/106685302446826652950?project=qwiklabs-gcp-00-f32d893dca78 t...
ResourcePath	["projects/qwiklabs-gcp-00-f32d893dca78/", "folders/623180826927/", "folders/874212290428/", "folders/365352270458/", "organizations/61646...
ScannerName	IAM_SCANNER



prerequisites before you run the lab
End Lab
01:09:33

Caution: When you are in the console, do not deviate from the lab instructions. Doing so may cause your account to be blocked. Learn more.

Open Google Cloud console

Google Cloud username 1

student-04-eeab9836b7fa

Google Cloud username 2

4. Which tab in the **User managed service account key** page provides compliance standards, explanation of the threat, and a recommendation on how to handle the threat?

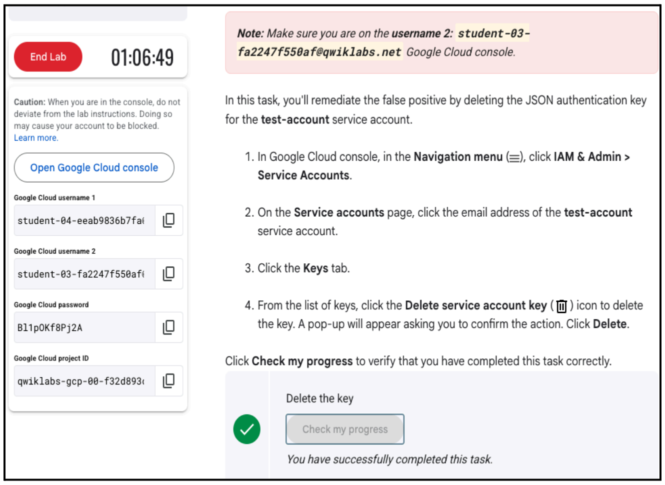
○ JSON

✓ Summary

✗ ~~Source Properties~~

Task 6: Fix the finding

In this final task, I used Identity and Access Management to delete the key.



Caution: When you are in the console, do not deviate from the lab instructions. Doing so may cause your account to be blocked. Learn more.

Google Cloud username 1
student-04-eeab9836b7fa

Google Cloud username 2
student-03-fa2247f550af

Google Cloud password
Bl1pOKf8Pj2A

Google Cloud project ID
qwiklabs-gcp-00-f32d893

***Note:** Make sure you are on the **username 2:** `student-03-fa2247f550af@qwiklabs.net` Google Cloud console.*

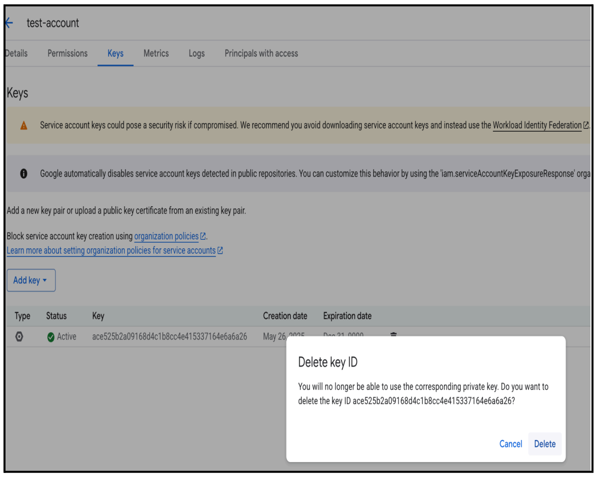
In this task, you'll remediate the false positive by deleting the JSON authentication key for the **test-account** service account.

1. In Google Cloud console, in the **Navigation menu** (≡), click **IAM & Admin > Service Accounts**.
2. On the **Service accounts** page, click the email address of the **test-account** service account.
3. Click the **Keys** tab.
4. From the list of keys, click the **Delete service account key** (🗑) icon to delete the key. A pop-up will appear asking you to confirm the action. Click **Delete**.

Click **Check my progress** to verify that you have completed this task correctly.

Delete the key

You have successfully completed this task.



Keys

Service account keys could pose a security risk if compromised. We recommend you avoid downloading service account keys and instead use the Workload Identity Federation.

Google automatically disables service account keys detected in public repositories. You can customize this behavior by using the 'iam.serviceAccountKeyExposureResponse' orga

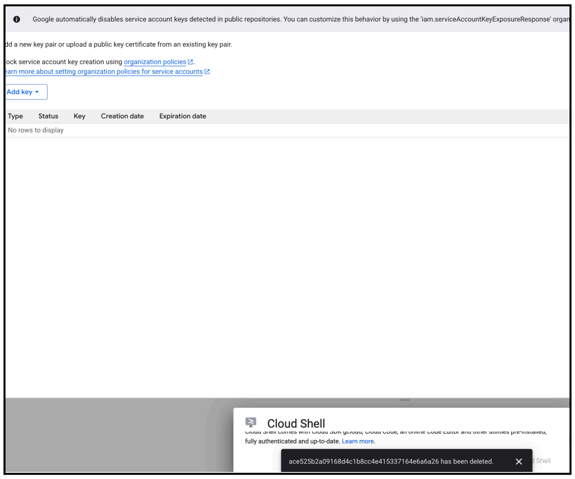
Add a new key pair or upload a public key certificate from an existing key pair.

Block service account key creation using organization policies.
Learn more about setting organization policies for service accounts

Type	Status	Key	Creation date	Expiration date
	✓ Active	ace525b2a09168d4c1b8cc4e415337164e6a6a26	May 26, 2025	Dec 31, 9999

Delete key ID

You will no longer be able to use the corresponding private key. Do you want to delete the key ID ace525b2a09168d4c1b8cc4e415337164e6a6a26?



Google automatically disables service account keys detected in public repositories. You can customize this behavior by using the 'iam.serviceAccountKeyExposureResponse' organ

dd a new key pair or upload a public key certificate from an existing key pair.

ock service account key creation using organization policies.
earn more about setting organization policies for service accounts

Type	Status	Key	Creation date	Expiration date
No rows to display				

Cloud Shell
fully authenticated and up-to-date. Learn more.

ace525b2a09168d4c1b8cc4e415337164e6a6a26 has been deleted.

My Assessment

In this lab I used various GCP services to trigger and fix a false positive. Primarily using Identity and Access Management (IAM), I was able to create a legitimate user test account, assign excessive permissions, which triggered a threat that I was able to also fix.

A false positive is essentially a positive alert based on the security parameters set within the system, however, there isn't an active threat due to authorized permissions granted.

False positives, if happening excessively, can cause a waste of resources, alert fatigue, disruption and potentially overlooking real threats. False positives may rely on pattern recognition or static rules that will often trigger an abundance of false positives.