Navigate the Security Center

Introduction to Exercise

The Security center gives you a security dashboard and security health recommendations. The security center brings together security analytics, actionable insights and best practice recommendations from Google to empower you to protect your organization, data and users.

• See the Security Center articles to learn more.

Exercise Scenario

In this exercise, you'll navigate to the security center to view and understand your security dashboard and security health recommendations.

Exercise Directions

Access the Security Center dashboard

1. Sign into your Cloud Identity Admin Console as the administrator user using **your administrator account name and password.**

2. Click the **Security icon**.

3. Click on **Dashboard**. From here, you can get overview of key security metrics for:

Failed device login attempts — This report will show you details of failed login attempts on your corporate devices during a specified time range

Note: *See the Failed device login attempts report article to learn more.*

Compromised device events — This report will show you details of compromised device events.

Note: *Use this report to view device IDs, device owners, and the timestamps of compromised devices. See the Compromised device events report article to learn more.*

Suspicious device activities — What suspicious device activities have been detected? Details of suspicious activities on your corporate devices during a specified time range

Note: *Use this report to view device IDs, device owners, and the timestamps of the suspicious device activities. See the Suspicious device activities report article to learn more.*

OAuth grant activity report — This report is ranked by the growth in grants to apps in the current time period compared to the previous time period.

Note: *Use this report to monitor the OAuth grant activity in your organization by app, scope, or user. See the OAuth grant activity report article to learn more.*

OAuth grants to new apps report—This report shows the new apps that have been provided OAuth grants in the given time period compared to the previous similar time period.

Note: *Use this report to monitor the OAuth grant activity in your organization. See the OAuth grants to new apps report article to learn more.*

See Security dashboard to learn more**.**

Access the Security Center health page

1. From the **Admin console dashboard**, click the **Security icon**

2. Click on **Security health**. The security health page enables you to monitor the configuration of your Admin console settings and stay ahead of potential threats by examining security analytics and flagging threats.

• From here you can monitor the security health of the following settings:

Device management settings - you can monitor the configuration of the following Device management settings:

- Mobile management
- Blocking of compromised mobile devices
- Mobile password requirements
- Device encryption
- Mobile inactivity reports
- Auto account wipe for Android
- Mobile application verification for Android
- Installation of mobile applications from unknown sources

- External media storage

Security settings - you can monitor settings related to security and protection of user accounts:

- 2-step verification for users
- 2-step verification for admins
- Security key enforcement for users

See Get started with the security health page to learn more.

Congratulations! You now know how to access the Security center to view and understand your dashboard and health recommendations.

See Security dashboard to learn more.

Revision #1
Created 2026-02-10 01:15:54 UTC by joliveira
Updated 2026-02-10 01:16:10 UTC by joliveira