>

This page walks you through accessing Security Command Center findings to review possible security risks, called *findings*, for your organization's Google Cloud, hybrid, and multi-cloud resources.

To access Security Command Center findings, you must have a Cloud Identity and Access Management (Cloud IAM) role that includes the permissions of the **Security Center Findings Viewer** role.

For more information about Security Command Center Cloud IAM roles, see Access control (/security-command-center/docs/access-control).

1. Go to the **Security Command Center** in the Cloud Console.

   Go to the Security Command Center (https://console.cloud.google.com/security/command-center/dashboard)
2. Select the organization you want to review.
3. On the Security Command Center dashboard that appears, click the **Findings** tab.

You're now viewing the Security Command Center findings detailed list view.

The Security Command Center Findings display enables you to view potential security risks for your organization.

Findings inventory freshness depends on finding sources:

- Finding freshness in the Security Command Center dashboard is usually <1 minute after ingestion from the finding source.
- Assets that haven't been discovered and indexed in an automatic or manual scan will usually appear in the findings inventory within 1 minute after discovery.

By default, findings are displayed in specific categories like cross-site scripting (XSS) and exposure of credit card number or phone number. If you leave the category field blank when you create a finding, it doesn't have a category in the Findings display.

- To view details about a specific risk type, under **View by Finding type**, select the type of risk you want to review. All findings of that type are displayed in the middle panel.
- To view detailed information about a specific finding, click the finding under `category`.

A finding source is any provider of findings, like Web Security Scanner or Cloud DLP Data Discovery scanner. These sources include the following:

- Scanners that provide a sampled snapshot of findings at a specific time.
- Monitors that provide an event stream of findings.
- Loggers that provide output of historical events.

You can view findings by source in multiple ways:

- To view findings grouped by source type, under the **Findings tab**, click **Source type**.
- To view individual findings for a specific source type, under **View by Source type**, select the source type you want to review. All findings of that type are displayed in the middle panel.
- To view detailed information about a specific finding, click the finding under `category`.

To view new and inactive findings, under the **Findings** tab, click **Findings changed**. All findings are displayed in the following subgroups:

- Active changed findings: findings that changed to active during the selected time period.
- Active unchanged findings: findings that are active and were active during all or part of the selected time period.
- Inactive changed findings: findings that changed to inactive during the selected time period.
- Inactive unchanged findings: findings that are inactive and were inactive during the selected time period.
- New findings: findings that are new during the selected time period.

Any findings in a group with a "Changed" tag have changed properties during the selected time range.

You can specify a time range for which results are displayed by clicking the drop-down list at the top of the findings list.

Manage security marks (/security-command-center/docs/how-to-security-marks) for findings or change finding state by using the **Info Panel** on the Security Command Center dashboard.

To add security marks to findings:

1. Under `category`, select one or more findings.
2. On the **Info Panel**, under **SecurityMarks**, click **Add mark**.
3. Add **Key** and **Value** items to identify the finding categories.

   For example, if you want to mark findings that are part of the same incident, add a key of "incident-number" and a value of "1234". Each finding will then have the new `mark.incident-number: 1234`.
4. When you're finished adding marks, click **Save**.

To remove security marks from findings:

1. Under `category`, select one or more findings.
2. On the **Info Panel**, under **SecurityMarks**, click **remove**. ✕

Change finding state to active or inactive by using the **Info Panel** on the Security Command Center dashboard:

1. Under `category`, select one or more findings.
2. On the **Info Panel**, under **Actions**, select **Active** or **Inactive** on the **State** drop-down list.
3. When you're finished changing finding state, click **Save**.

By default, the findings tab displays the following columns:

- Finding type: `category`
- Asset ID: `resourceName`
- Time the finding was last detected: `eventTime`
- Time the finding was first detected: `createTime`
- The source of the finding: `parent`
- Any marks added to the finding: `securityMarks.marks`

You can hide any column except for `category`, and you can select more finding detail columns to display.

1. To select the finding columns you want to display, click **Columns**. ▮▮▮
2. In the menu that appears, select the columns you want to display.
3. To hide a column, click the column name.

To save your column selections, click **Remember Columns**. Your column selections apply to all of the views in the **Findings** tab. When you select columns, the Cloud Console URL updates, so you can share the link for a custom view.

Column selections are preserved the next time you view the dashboard, and if you change organizations. To clear all custom column selections, click **Reset Columns**.

To control the screen space for findings, you can change the following options:

- Hide the Cloud Console **Security** side panel by clicking the left arrow. <|
- Resize the findings display columns by dragging the dividing line left or right.
- Hide the **Select a finding** side panel by clicking **Hide Info Panel**.

To change the date and time for which the findings tab displays results, click the date and time drop-down, then select the date and time you want.

- Learn how to Security Command Center use security marks (/security-command-center/docs/how-to-security-marks).
- Learn more about Security Command Center (/security-command-center/docs/concepts-overview).

- Learn how to use the assets display (/security-command-center/docs/how-to-assets-display).