

This page walks you through accessing Security Command Center, configuring the display, and reviewing your Google Cloud resources. If Security Command Center is not already set up for your organization, complete the [Quickstart: Setting up Security Command Center](/security-command-center/docs/quickstart-scc-setup) (/security-command-center/docs/quickstart-scc-setup) first.

To use Security Command Center, you must have a Cloud Identity and Access Management (Cloud IAM) role that includes appropriate permissions:

- To view Security Command Center, you must have the **Security Center Admin Viewer** Cloud IAM role.
- To make changes to Security Command Center, you must have an appropriate editor role, like **Security Center Admin Editor**.

If your organization policies are set to [restrict identities by domain](/resource-manager/docs/organization-policy/restricting-domains) (/resource-manager/docs/organization-policy/restricting-domains), you must be signed in to the Cloud Console on an account that's in an allowed domain.

Learn more about [Security Command Center roles](/security-command-center/docs/access-control) (/security-command-center/docs/access-control).

This section walks through accessing Security Command Center and viewing Assets and Findings for your Google Cloud resources.

To access the Security Command Center dashboard:

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

[Go to the Security Command Center page](https://console.cloud.google.com/security/dashboard) (https://console.cloud.google.com/security/dashboard)

2. Select the organization you want to review.

The Security Command Center dashboard displays a basic overview of potential security risk findings. The dashboard includes the summary cards described below.

Assets are the Google Cloud resources for your organization. The **Assets Summary** card displays a count of each type of asset in your organization as of the most recent scan. The display includes new, deleted, and total assets for the time period you specify. You can view the summary as a table or a graphical chart.

- To view the summary for a recent time range, select one from the drop-down list on the **Assets** card.
- To view the summary for a specific date and time, click **View all assets**, and then select the date and time on the time drop-down list.
- To view your organization's tree hierarchy, click an asset type or **View all assets**.
- To view details about an individual asset, select the Assets tab, and then click the asset name.

Learn more about [Using the Assets display](/security-command-center/docs/how-to-assets-display/) (/security-command-center/docs/how-to-assets-display).

Findings are possible security risks. The **Findings Summary** card displays a count of each category of finding that the enabled finding sources provide.

- To view details about the findings from a specific source, click the source name.
- To view details about all findings, select the **Findings** tab.

On the Findings tab, you can group Findings or view details. Grouping by source type can help you identify which detector is the source. You can also group by detection category type, like cross-site scripting (XSS) or coin-mining.

- To group Findings, toggle between **View by** options.
- To view details about findings in a specific category, click the name under **category**.

Learn more about [Using Findings](/security-command-center/docs/how-to-findings/) (/security-command-center/docs/how-to-findings).

This section describes how to run common queries to review your resources using Security Command Center.

You can only select these filters in the Security Command Center dashboard if your organization has the related resource type. If you receive the "Choose one of the suggested keys" error message, your organization might not have that resource type.

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

[Go to the Assets page \(https://console.cloud.google.com/security/assets\)](https://console.cloud.google.com/security/assets)

2. In the **Filter by** text box:

- a. Type `resourceProperties.acl:allUsers`, and then press **Enter**.
- b. Click the **Filter by** text box, and then select **OR** on the drop-down list.
- c. Type `resourceProperties.acl:allAuthenticatedUsers`, and then press **Enter**.

The following filter finds firewall rules with SSH port 22 open from any network.

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

[Go to the Assets page \(https://console.cloud.google.com/security/assets\)](https://console.cloud.google.com/security/assets)

2. In the **Filter by** text box:

- a. Type `resourceProperties.allowed:22`, and then press **Enter**.
- b. Click the **Filter by** text box, and then select **OR** on the drop-down list.
- c. Type `resourceProperties.sourceRange:0.0.0.0/0`, and then press **Enter**.

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

[Go to the Assets page](https://console.cloud.google.com/security/assets) (https://console.cloud.google.com/security/assets)

2. In the **Filter by** text box, enter `resourceProperties.networkInterface:externalIP`.

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

[Go to the Assets page](https://console.cloud.google.com/security/assets) (https://console.cloud.google.com/security/assets)

2. In the **Filter by** text box, enter -
`securityCenterProperties.resourceOwners:[YOUR_DOMAIN]`.

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

[Go to the Assets page](https://console.cloud.google.com/security/assets) (https://console.cloud.google.com/security/assets)


2. In the **Filter by** text box, enter `resourceProperties.disk:licenses`.
3. On the list of displayed resources, click **Column display options**, and then select **resourceProperties.disk**.

In Security Command Center settings, you can configure monitoring, permissions, and security sources. To access settings, click **Settings** on the Security Command Center dashboard, and then select the tab you want to configure.

By default, Security Command Center discovers assets within each project during asset discovery. On the **Asset Monitoring** tab, you can include or exclude specific projects to be scanned for asset discovery. To configure asset monitoring select one of the available options:

- **All current and future projects:** the default state in which assets within all your projects are scanned for asset discovery.
- **Include projects:** select specific projects that will be scanned for asset discovery.
- **Exclude projects:** select specific projects that won't be scanned for asset discovery.

After you save changes to Asset Monitoring, asset discovery will run and refresh the Assets display.

On the **Permissions** tab, you can view and configure Cloud IAM roles for Security Command Center. You can list permissions by **Members** or by **Roles**. To add or remove Security Command Center Cloud IAM roles for a user, click **Edit** . In the **Edit permissions** panel that appears, add or remove roles.

Security sources provide vulnerability and threat data in the Security Command Center dashboard. Security Command Center includes default sources like Anomaly Detection, Web Security Scanner, and Cloud DLP Data Discovery. On the **Security Sources** tab, you add new sources or enable and disable existing ones.

Each security source uses a service account that might be outside your organization. If your organization policies are set to [restrict identities by domain](#) (</resource-manager/docs/organization-policy/restricting-domains>), you also need to add the service account to an identity in a group that's within an allowed domain. For more information, see [Adding vulnerability and threat sources](#) (</security-command-center/docs/how-to-security-sources>).

- Learn about [using the assets display](#) (</security-command-center/docs/how-to-assets-display>) to review details like project owners and organize your assets using marks.
- Learn how to [use findings](#) (</security-command-center/docs/how-to-findings>) to understand details about your potential security risks.

- Learn about native Google Cloud scanners and how to view the vulnerabilities and threats (</security-command-center/docs/how-to-view-vulnerabilities-threats>) they surface.
- Learn how to add security sources to Security Command Center (</security-command-center/docs/how-to-security-sources>).