Use Security Command Center in the Google Cloud console

Archived: 2026-04-05 23:12:20 UTC

This page provides an overview of Security Command Center in the Google Cloud console, describes the navigation, and gives an overview of top-level pages.

If you haven't set up Security Command Center, see one of the following for instructions about how to activate it:

- To activate the Standard or Premium tier, see Overview of activating Security Command Center.
- To activate the Enterprise tier, see Activate the Security Command Center Enterprise tier.

For a general overview of Security Command Center, see Security Command Center overview.

If Security Command Center was recently activated, it might take time for data to appear. For information about the scan frequency of Security Command Center services, see When to expect findings in Security Command Center.

Required IAM permissions

To use Security Command Center with all service tiers, you must have an Identity and Access Management (IAM) role that includes appropriate permissions:

- **Security Center Admin Viewer** (`roles/securitycenter.adminViewer`) lets you view Security Command Center.
- **Security Center Admin Editor** (`roles/securitycenter.adminEditor`) lets you view Security Command Center and make changes.

You must have one of the following:

- **Security Center Admin** (`roles/securitycenter.admin`)
- **Security Center Admin Editor** (`roles/securitycenter.adminEditor`)
- **Security Center Viewer** (`roles/securitycenter.adminViewer`)

- **Security Center Admin Viewer** (`roles/securitycenter.adminViewer`) lets you view Security Command Center.
- **Security Center Admin Editor** (`roles/securitycenter.adminEditor`) lets you view Security Command Center and make changes.

- **Security Center Admin Viewer** (`roles/securitycenter.adminViewer`) lets you view Security Command Center.
- **Security Center Admin Editor** (`roles/securitycenter.adminEditor`) lets you view Security Command Center and make changes.
- **Chronicle Service Viewer** (`roles/chroniclesm.viewer`) lets you view the associated Google SecOps instance.

You also need any of the following IAM roles:

- **Chronicle SOAR Admin** (`roles/chronicle.soarAdmin`)
- **Chronicle SOAR Threat Manager** (`roles/chronicle.soarThreatManager`)
- **Chronicle SOAR Vulnerability Manager** (`roles/chronicle.soarVulnerabilityManager`)

To enable access to SOAR-related features, you must also map these Identity and Access Management roles to a **SOC role**, **Permission group**, and **Environment** on the **Settings > SOAR settings** page. For more information, see Map and authorize users using IAM.

If your organization policies are set to restrict identities by domain, you must be signed in to the Google Cloud console on an account that's in an allowed domain.

The IAM roles for Security Command Center can be granted at the organization, folder, or project level. Your ability to view, edit, create, or update findings, assets, and security sources depends on the level for which you are granted access. To learn more about Security Command Center roles, see Access control.

To access Security Command Center in the Google Cloud console:

1. Go to Security Command Center:

   Go to Security Command Center

   If data residency is enabled and your organization uses the jurisdictional Google Cloud console, see About the jurisdictional Google Cloud console.

2. Select the project or organization that you want to view.

   If Security Command Center is active in the organization or project you select, the **Risk overview** page appears.

   If Security Command Center is not active, you are invited to activate it. For more information about activating Security Command Center, see one of the following:

   - Standard, Standard-legacy, or Premium: Overview of activating Security Command Center.
   - Enterprise: Activate the Security Command Center Enterprise tier.

Security Command Center navigation

The following describes the navigation in Security Command Center. The navigation differs depending on your Security Command Center service tier. The tasks that you can perform also depend on services that are enabled and the IAM permissions that you are granted.

Click a link for an explanation of the page.

The following describes the navigation in Security Command Center Standard-legacy service tier.

- Risk overview

- Issues page: Prompts you to upgrade to the Premium service tier.
- Threats: Prompts you to upgrade to the Premium service tier.
- Compliance: Prompts you to upgrade to the Premium service tier.
- Assets
- Findings
- Sources
- Posture Management: Prompts you to upgrade to the Premium service tier.
- Settings

The following describes the navigation in Security Command Center Standard.

- Risk overview
- Issues page: Prompts you to upgrade to the Premium service tier.
- Threats: Prompts you to upgrade to the Premium service tier.
- Compliance
- Assets
- Findings
- Sources
- Posture Management: Prompts you to upgrade to the Premium service tier.
- Settings

The following describes the navigation in Security Command Center Premium.

- Risk overview
- Graph Search
- Issues page
- Findings
- Assets
- Compliance
- Posture Management
- Sources
- Settings

In the Security Command Center Enterprise left navigation, **Cases** links to pages in the Google Security Operations tenant that was configured during Security Command Center Enterprise activation.

For information about the features available in Google Security Operations, see Security Command Center Enterprise links to the Security Operations console.

- Risk overview
- Graph Search
- Issues page
- Findings
- Assets
- Compliance

- Posture Management
- Sources
- Settings
- Setup Guide
- Cases

Risk overview

The **Risk overview** page serves as your first-contact security dashboard, highlighting high-priority risks in your cloud environments identified by all built-in and integrated services.

The views on the **Risk overview** page differ depending on your service tier.

Learn more about each investigative view by selecting one of the following views:

- All risk: shows misconfiguration findings.
- Vulnerabilities: displays vulnerabilities and related CVE information.
- Identity: shows a summary of identity and access findings by category.
- Threats: Prompts you to upgrade to the Premium service tier.

Learn more about each investigative view by selecting one of the following views:

- All risk: shows misconfiguration findings.
- Vulnerabilities: displays vulnerabilities and related CVE information.
- Identity: shows a summary of identity and access findings by category.
- Data: displays information about your data security posture.
- Threats: Prompts you to upgrade to the Premium service tier.

Learn more about each investigative view by selecting one of the following views:

- All risk: shows all data.
- Vulnerabilities: displays vulnerabilities and related CVE information.
- Identity: shows a summary of identity and access findings by category.
- Data: displays information about your data security posture.
- AI Security: shows AI-related findings and security posture data.
- Threats: shows threat-related findings.

Learn more about each investigative view by selecting one of the following views:

- All risk: shows all data.
- Vulnerabilities: displays vulnerabilities and related CVE information.
- Identity: shows a summary of identity and access findings by category.
- Data: displays information about your data security posture.
- AI Security: shows AI-related findings and security posture data.
- Threats: shows threat-related findings.

Assets

The **Assets** page provides a detailed display of all Google Cloud resources, also called *assets*, in your project or organization.

For more information about how to work with assets on the **Assets** page, see Work with resources in the console.

Compliance

By default, when you activate Security Command Center, you enable Compliance Manager. The **Compliance** page shows the following tabs: **Configure (New)**, **Monitor (New)**, and **Audit (New)**. These tabs let you create and apply cloud controls and frameworks, monitor your environment, and complete audits.

If you activated Security Command Center before Compliance Manager was generally available and you don't enable Compliance Manager, the **Compliance** page shows a **Monitor** tab only. This tab shows all industry benchmarks that Security Command Center supports using Security Health Analytics and the percentage of passing benchmark controls. For more information about how Security Command Center supports compliance management if Compliance Manager isn't enabled, see Assess compliance without Compliance Manager.

Findings

On the **Findings** page, you can query, review, mute, and mark Security Command Center *findings*, the records that Security Command Center services create when they detect a security issue in your environment. For more information about how to work with findings on the **Findings** page, see Review and manage findings.

Graph Search

Security graph in Security Command Center is a database that understands and maps the relationships between your cloud resources, their configurations, and associated security risks. These risks include vulnerabilities, access permissions, data sensitivity, and network exposure. This graph offers a comprehensive view of your cloud assets and their interdependencies.

On the **Graph Search** page, you can query the Security graph to proactively identify and monitor potential security vulnerabilities within your environment.

Issues

Issues are the most important security risks that Security Command Center finds in your cloud environments, giving you the opportunity to respond quickly to vulnerabilities and threats. Security Command Center discovers issues through virtual red teaming and rule-based detections. For information about investigating issues, see Issues overview.

Posture management

On the **Posture** page, you can view details about the security postures that you created in your organization and apply the postures to an organization, folder, or project. You can also view the available predefined posture

templates.

Settings

Open the **Settings** page from the **Settings** link in the navigation. The **Settings** page lets you configure Security Command Center, including the following:

- Additional Security Command Center services
- Multi-cloud connectors
- High-value resource sets
- Mute findings rules
- Continuous data exports

SCC setup guide

The **Setup guide** page lets you activate Security Command Center Enterprise and configure additional services. For more information, see Activate the Security Command Center Enterprise tier.

Sources

The **Sources** page contains cards that provide a summary of assets and findings from the security sources you have enabled. The card for each security source shows some of the findings from that source. You can click the finding category name to view all findings in that category.

Findings by source

The **Findings by source** card displays a count of each category of finding that your enabled security sources provide.

- To view details about the findings from a specific source, click the source name.
- To view details about all findings, click the **Findings** page, where you can group findings or view details about an individual finding.

Source summaries

Below the **Findings by source** card, separate cards appear for any built-in, integrated, and third-party sources you enabled. Each card provides counts of active findings for that source.

Threats

Threats are potentially harmful events in your cloud resources. Security Command Center displays threats in different views, depending on your service tier.

The **Threats** page is not supported in Security Command Center Standard and Standard-legacy. You can view threat findings on the **Findings** page.

In Security Command Center Premium, the **Threats** navigation link opens the **Risk Overview** > Threats dashboard.

In Security Command Center Enterprise, you view threats in the **Risk Overview** > Threats dashboard.

Legacy Vulnerabilities page

The legacy **Vulnerabilities** page lists all of the misconfiguration and software vulnerability findings that the built-in detection services of Security Command Center run in your cloud environments. For each listed detector, the number of active findings is displayed.

To view the **Vulnerabilities** page in Security Command Center, do the following:

1. In the Google Cloud console, go to the **Risk overview** page.

   Go to Risk overview

2. On the **Risk Overview** page, click **Vulnerabilities**.

3. On the **Vulnerabilities** dashboard, click **Go to legacy page**.

Vulnerability detection services

The **Vulnerabilities** page lists detectors for the following built-in detection services of Security Command Center:

- Notebook Security Scanner (Preview)
- Security Health Analytics
- Vulnerability Assessment for Amazon Web Services (AWS)
- Web Security Scanner

Other Google Cloud services that are integrated with Security Command Center also detect software vulnerabilities and misconfigurations. The findings from a selection of these services are also displayed on the **Vulnerabilities** page. For more information about the services that produce vulnerability findings in Security Command Center, see Detection services.

Information about vulnerability detector categories

For each misconfiguration or software vulnerability detector, the **Vulnerabilities** page shows the following information:

- **Status**: an icon indicates whether the detector is active and whether the detector found a finding that needs to be addressed. When you hold the pointer over the status icon, a tooltip displays the date and time the detector found the result or information about how to validate the recommendation.
- **Last scanned**: the date and time of the last scan for the detector.
- **Category**: the category or type of vulnerability. For a list of the categories that each Security Command Center service detects, see the following:
  - Notebook Security Scanner findings (Preview)

    - Security Health Analytics findings
    - Vulnerability Assessment for AWS findings
    - Web Security Scanner findings

- **Recommendation**: a summary of how to remediate the finding. For more information, see the following:

    - Remediating Security Health Analytics findings.
    - Remediating Web Security Scanner findings
    - Review and resolve package vulnerability findings

- **Active**: the total number of findings in the category.

- **Standards**: the compliance benchmark that the finding category applies to, if any. For more information about benchmarks, see Vulnerabilities findings.

Filtering vulnerability findings

A large organization might have many vulnerability findings across their deployment to review, triage, and track. By using filters that are available on the Security Command Center **Vulnerabilities** and **Findings** pages in the Google Cloud console, you can focus on the highest severity vulnerabilities across your organization, and review vulnerabilities by asset type, project, and more.

For more information about filtering vulnerability findings, see Filter vulnerability findings in Security Command Center.

Links to the Security Operations console

The Security Command Center Enterprise tier includes features available on both the Google Cloud console pages and on Security Operations console pages.

You sign in to the Google Cloud console and navigate to Security Operations console pages from the Google Cloud console navigation. This section describes the tasks that you can perform on each page and the navigation links that open Security Operations console pages.

For information about Google Security Operations features available with the Security Command Center Enterprise tier, see Google SecOps features in Security Command Center Enterprise.

The Google Cloud console pages let you perform tasks such as the following:

- Activate Security Command Center.
- Set up Identity and Access Management (IAM) permissions for all Security Command Center users.
- Connect to other cloud environments to collect resource and configuration data.
- Work with and export findings.
- Assess risks with attack exposure scores.
- Work with issues, the most important security risks Security Command Center Enterprise has found in your cloud environments.

- Identify high-sensitivity data with Sensitive Data Protection.
- Investigate and remediate individual findings.
- Configure Security Health Analytics, Web Security Scanner, and other Google Cloud integrated services.
- Manage security postures.
- Configure cloud controls and frameworks.
- Manage a data security posture.
- Assess and report on your compliance with common security standards or benchmarks.
- View and search your Google Cloud assets.

The Security Operations console page lets you perform tasks such as the following:

- Connect to other cloud environments to collect log data for curated detections in security information and event management (SIEM).
- Configure security orchestration, automation, and response (SOAR) settings.
- Configure users and groups for incident and case management.
- Work with cases, which includes grouping findings, assigning tickets, and working with alerts.
- Use an automated sequence of steps known as playbooks to remediate problems.
- Use Workdesk to manage actions and tasks waiting for you from open cases and playbooks.

```
https://CUSTOMER_SUBDOMAIN.backstory.chronicle.security/cases
```

Where `CUSTOMER_SUBDOMAIN` is your customer-specific identifier.

Cases

In the Security Operations console, you use cases to obtain details about findings, attach playbooks to finding alerts, apply automatic threat responses, and track the remediation of security issues.

For information, see Cases overview in Google Security Operations documentation.

What's next

- Learn about detection services.
- Learn how to use security marks.
- Learn how to configure Security Command Center services.
