

This page walks you through adding new vulnerability and threat sources, called *security sources*, to Security Command Center. In this context, a security source is a second or third-party security tool that provides security findings to Security Command Center.

You can add Google Cloud native security sources to Security Command Center along with other, third-party security tools. This enables you to have a complete view of your organization's security risks, vulnerabilities, and threats.

To add a new security source, you complete its integration guide, and then enable it as a security source in the Security Command Center dashboard.

Google Cloud offers the following native security sources that integrate with Security Command Center:

- [Security Health Analytics](/security-command-center/docs/how-to-enable-security-health-analytics) (/security-command-center/docs/how-to-enable-security-health-analytics)
- [Web Security Scanner](/security-scanner/docs/quickstart) (/security-scanner/docs/quickstart)
- [Anomaly Detection](/security-command-center/docs/how-to-view-vulnerabilities-threats#anomaly_detection) (/security-command-center/docs/how-to-view-vulnerabilities-threats#anomaly_detection)
- [Cloud Data Loss Prevention](/dlp/docs/sending-results-to-cscc) (/dlp/docs/sending-results-to-cscc)
- [Event Threat Detection](/event-threat-detection/) (/event-threat-detection/)
- [Forseti Security](https://forsetisecurity.org/docs/latest/configure/notifier/#cloud-scc-notification) (https://forsetisecurity.org/docs/latest/configure/notifier/#cloud-scc-notification)
- [Phishing Protection](/phishing-protection/docs/quickstart-console) (/phishing-protection/docs/quickstart-console)

Anomaly Detection findings are automatically available in Security Command Center. Findings from other native security sources are available after you complete their integration guides, linked in the preceding list. To view findings from security sources, you need to enable each security source in the Security Command Center dashboard.

Each security source uses a service account that might be outside your organization. For example, Google Cloud native security sources use a service account at `security-center-fpr.iam.gserviceaccount.com`. 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 need to add the service account to an identity in a group that's within an allowed domain.

On the **Security Sources** tab, you add new sources or enable and disable existing ones:

1. Go to the Security Command Center [Security Sources](https://console.cloud.google.com/security/command-center/settings/source-management) (https://console.cloud.google.com/security/command-center/settings/source-management) page in the Cloud Console.
[Go to the Security Sources page](https://console.cloud.google.com/security/command-center/settings/source-management) (https://console.cloud.google.com/security/command-center/settings/source-management)
2. Select the organization for which you want to add a security source.
3. Under **Enabled**, click to enable a security source.



Findings for the security sources you select are displayed on the Findings page in the Security Command Center dashboard.

Security Command Center can display findings from third-party security sources that have registered as a Google Cloud Marketplace partner. Third-party security partners that are already registered include the following:

- Acalvio
- Capsule8
- Cavin
- Chef
- Check Point CloudGuard Dome9
- Cloudflare
- CloudQuest
- McAfee
- Qualys
- Reblaze
- Redlock by Palo Alto Networks
- StackRox
- Tenable.io
- Twistlock

If you want to integrate a security source that isn't already registered as a Google Cloud Marketplace partner, ask your provider to complete the guide to [Onboard as a Security Command Center partner](/security-command-center/docs/how-to-partner-onboard) (/security-command-center/docs/how-to-partner-onboard).

To add a new third-party security source to Security Command Center, you set up the security source, and then enable it in the Security Command Center dashboard.

To add a security source for a registered Google Cloud Marketplace partner, you need:

- The following Cloud Identity and Access Management (Cloud IAM) [roles](/iam/docs/understanding-roles) (/iam/docs/understanding-roles):
 - Security Center Admin - `roles/securitycenter.admin`
 - Service Account Admin - `roles/iam.serviceAccountAdmin`
- A Google Cloud project that you want to use for the security source.

To set up a third-party security source, you need a service account for that source. When you add the new security source, you can choose from the following service account options:

- Create a service account.
- Use your own existing service account.

- Use a service account from the source provider.

To set up a new security source that's already registered as a Google Cloud Marketplace partner, follow the steps below:

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

[Go to the Marketplace page](https://console.cloud.google.com/marketplace/browse?filter=category:security-command-center-services) (https://console.cloud.google.com/marketplace/browse?filter=category:security-command-center-services)

2. The **Marketplace** page displays security sources that are directly associated with Security Command Center.
 - If you don't see the security source that you want to add, search for **Security**, and then select the security source provider.
 - If the security source provider isn't registered in the Google Cloud Marketplace, ask your provider to complete the guide to [Onboard as a Security Command Center partner](/security-command-center/docs/how-to-partner-onboard) (/security-command-center/docs/how-to-partner-onboard).
3. On the security source provider page in the Google Cloud Marketplace, follow any provider setup instructions in the **Overview**.
4. After you complete the provider's setup process, click **Visit [provider name] site to sign up** on the provider's **Marketplace** page.
5. On the Cloud Console **Security Command Center** page that appears, select the organization for which you want to use the security source.
6. On the **Create Service Account & Enable [provider name] Security Events** page that appears, accept the provider's service account, if available, or create or select your own service account that you want to use:
 - To create a service account:
 - a. Select **Create a new service account**.
 - b. Next to **Project**, click **Change** to select the project you want to use for this security source.
 - c. Add a **Service account name** and **Service account ID**.
 - To use an existing service account:
 - a. Select **Use an existing service account**, then select the service account you want to use from the **Service account name** drop-down list.
 - If the security source provider manages the service account, enter the **Service account ID** they provided.
7. When you're finished adding service account information, click **Submit** or **Accept**.
8. On the **Source connect** page that appears, click the link under **Installation Steps** for information about how to complete installation.
9. When you're finished, click **Done**.

When configured correctly, the security source you added is available in Security Command Center.

After you set up a new security source, you need to enable it in the Security Command Center dashboard.

Each security source uses a service account that might be outside your organization. For example, Google Cloud native security sources use a service account at `security-center-fpr.iam.gserviceaccount.com`. 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 need to add the service account to an identity in a group that's within an allowed domain.


On the **Security Sources** tab, you add new sources or enable and disable existing ones:

1. Go to the Security Command Center [Security Sources](https://console.cloud.google.com/security/command-center/settings/source-management) (<https://console.cloud.google.com/security/command-center/settings/source-management>) page in the Cloud Console.
[Go to the Security Sources page](https://console.cloud.google.com/security/command-center/settings/source-management) (<https://console.cloud.google.com/security/command-center/settings/source-management>)
2. Select the organization for which you want to add a security source.
3. Under **Enabled**, click to enable a security source.



Findings for the security sources you select are displayed on the Findings page in the Security Command Center dashboard.

You can change the service account used for a third-party security source, for example to address service account leakage or rotation. To change the service account for a security source, you need to update it in the Security Command Center dashboard, and then follow the service provider's instructions to update the service account for their service.

1. Go to the Security Command Center **Security Sources** page in the Cloud Console.
[Go to the Security Sources page](https://console.cloud.google.com/security/command-center/settings/source-management) (<https://console.cloud.google.com/security/command-center/settings/source-management>)
2. Under **Enabled**, click to temporarily disable the security source for which you want to change the service account.
3. Next to the service account name, click **Edit**. 
4. On the **Edit [provider name]** panel that appears, enter the new service account, then click **Submit**.
5. Under **Enabled**, click to enable the security source.



When configured correctly, the service account for the security source is updated in Security Command Center. You must also follow the source provider's instructions to update the service account information for their service.

- Learn about native Google Cloud scanners and how to [view the vulnerabilities and threats](https://cloud.google.com/security-command-center/docs/how-to-view-vulnerabilities-threats) (/security-command-center/docs/how-to-view-vulnerabilities-threats) they surface.