This page describes how to set up Security Command Center for your organization for the first time. If Security Command Center is already set up for your organization, go to Using the dashboard (/security-command-center/docs/quickstart-scc-dashboard).

The following video shows the steps to set up Security Command Center, and provides information about how to use the dashboard. The setup steps are described in text later on this page.

If your organization policies are set to restrict identities by domain (/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;
- Your service accounts must be in an allowed domain, or members of a group within your domain. This enables you to allow `@*.gserviceaccount.com` services access to resources when domain restricted sharing is enabled.

If you're using VPC Service Controls, you must grant access (/access-context-manager/docs/create-access-level#members-example) to the Security Command Center service account after you enable Security Command Center.

To set up Security Command Center for your organization, you add necessary Cloud Identity and Access Management (Cloud IAM) roles, enable the Security Command Center dashboard, and then enable security sources to display findings in the Security Command Center dashboard.

To set up Security Command Center for your organization for the first time, you need the following Cloud Identity and Access Management roles that include appropriate permissions:

- **Organization Administrator** role - `roles/resourcemanager.organizationAdmin`. Learn more about managing organizations (/resource-manager/docs/creating-managing-organization).
- **Security Center Admin** role - `roles/securitycenter.admin`. Add this role for yourself even if you're the organization owner.

To add these roles:

1. Go to the IAM & Admin (https://console.cloud.google.com/iam-admin/iam) page in the Cloud Console.

   Go to the IAM & Admin page (https://console.cloud.google.com/iam-admin/iam)

2. Click the **Project selector** drop-down list at the top of the page.
3. On the **Select from** dialog that appears, select the organization for which you want to enable Security Command Center.
4. On the **IAM** page, next to your username, click **Edit**. ✏
5. On the **Edit permissions panel** that appears, add the necessary roles:
    a. Click **Add another role**. Select **Resource Manager > Organization Administrator**. If you don't have permissions to add the role, ask your organization super admin to grant you the role.

    b. Click **Add another role**. Select **Security Center > Security Center Admin**.

    c. When you're finished adding roles, click **Save**.

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

1. Go to the Security Command Center (https://console.cloud.google.com/security/command-center/welcome) page in the Cloud Console.

    Go to the Security Command Center page (https://console.cloud.google.com/security/command-center/welcome)
2. On the **Organization** drop-down list, select the organization for which you want to enable Security Command Center, and then click **Select**.
3. On the **Enable asset discovery** page that appears, select **All current and future projects**, and then click **Enable**.
    - A message might display that you must have the Security Center Admin and Organization Admin roles. If you already have these roles:

        a. Check if your organization policies restrict identities by domain (/resource-manager/docs/organization-policy/restricting-domains);

        b. Make sure you sign in to an account that's in an allowed domain.
    - If you're using an `@*.gserveraccount.com service` account, add the service account as an identity in a group within an allowed domain.
4. If you're using VPC Service Controls, grant access (/access-context-manager/docs/create-access-level#members-example) to the Security Command Center service account. This allows the service account to complete asset discovery and display assets in the Security Command Center dashboard. The service account name is in the form of `service-org-organization-id@security-center-api.iam.gserviceaccount.com`.

When your service account is in an allowed domain and you have granted VPC Service Controls access, Security Command Center will begin asset discovery.

After asset discovery is complete, Security Command Center will display your supported Google Cloud assets. Asset discovery might take a few minutes, and you might need to refresh the page to display the assets.

To view findings in the Security Command Center dashboard, you need to enable the security scanners you're using as security sources. Anomaly Detection (/security-command-center/docs/how-to-view-vulnerabilities-threats#anomaly_detection) findings are automatically available. Web Security Scanner findings are available if you've completed the Web Security Scanner quickstart (/security-scanner/docs/quickstart).

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), 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) page in the Cloud Console.

   Go to the Security Sources page (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.

- For more information about native Google Cloud scanners and the findings they surface, see viewing the vulnerabilities and threats (/security-command-center/docs/how-to-view-vulnerabilities-threats).
- If you add new security sources (/security-command-center/docs/how-to-security-sources) later, you need to repeat the preceding process to view findings for the new source.

- Learn how to use the Security Command Center dashboard (/security-command-center/docs/quickstart-scc-dashboard).
- 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).