>

This page provides information about how to prepare your Google Cloud project to install the Security Command Center tools app package. These apps add new functionality that show how you can use Security Command Center in your organization.

These apps demonstrate how to develop integrations or add-ons to the Security Command Center platform. If you're a third-party security solution developer, or if you need something more specific for your organization, you might find these example apps particularly useful.

The Security Command Center tools package includes the following components:

Hello World is a small app that calls the Security Command Center API to get an organization's assets or security provider findings. This app uses Cloud Functions to integrate with Security Command Center APIs and trigger security workflows based on Security Command Center queries:

- Log query parameters and results.
- Disable firewall rules that allow SSH connections to an instance.
- Remove access to a Cloud Storage bucket.
- Create a snapshot for each disk that belongs to an instance.

Hello World also includes a small library of example Cloud Functions that enable you to programmatically trigger the following actions with Pub/Sub messages:

- Repair firewall
- Snapshot VM
- Change bucket ACL

You can use the Hello World app code as a starting point for other behaviors like:

- Use Cloud Scheduler to periodically call a Pub/Sub topic and trigger a security workflow.
- Store query results in a database or send it to another system as a notification.
- Add a new Cloud Functions function to call another Google API.

The Creator app queries Security Command Center data at regular intervals and sends the results to a Notifications Pub/Sub Topic. The Creator app provides examples of how to use the `filter`, `readTime`, and `compareDuration` parameters of the Security Command Center API (/security-command-center/docs/reference/rest/).

The Query Builder app enables you to create and schedule advanced, multi-step queries on Security Command Center data using a web application interface. Query results can be sent to a Notifications Pub/Sub Topic where other apps can consume them. You can also configure Query Builder to add Security Command Center security marks to query results.

For example, you could schedule a query to periodically look for network firewalls with port 22 allowed. You could then use Query Builder to mark the results in Security Command Center and notify your security team so they can take appropriate action.

The Notifier app subscribes to a Notifications Pub/Sub Topic and sends notifications to a configured channel, like email or SMS. The Notifier app refers to Security Command Center query results from other apps, like the Creator and Query Builder apps.

You can develop your own application to subscribe to the same Notifications Pub/Sub Topic, and customize how you handle the messages you get. For example, you could process the results and send them to one of your organization's internal systems, or store the results for further analysis in a database that you specify.

The Audit Logs app can ingest Cloud Audit Logs logs through export sinks and create Security Command Center security findings. This app includes integration of Access Transparency alerts and Binary Authorization alerts for Blocked Deployments and Break Glass scenarios. The Audit Logs app is a streaming Dataflow job. Using the Audit Logs app incurs charges per Dataflow pricing (/dataflow/pricing).

This app creates *single* and *aggregated* log types:

- Single log types create a Security Command Center finding for each occurrence found:
    - Google Kubernetes Engine Binary Authorization
    - Access Transparency
    - Compute Engine
    - Cloud Storage
    - Service Networking
- Aggregated log types group findings within a Dataflow period and then creates a Security Command Center finding:
    - Cloud Identity and Access Management (Cloud IAM)

The Splunk Connector app uses the Security Command Center API to export an organization's assets and findings. You can configure the app to filter Security Command Center data to limit the data that's exported. For example, you could search for only findings of a specific type. The app runs on a schedule and delivers results to a Pub/Sub Topic that's connected to a Splunk Server Addon.

The Security Command Center tools package includes a set of companion scripts and utilities. The scripts and utilities are used during installation to create the necessary Google Cloud infrastructure for each app and help deploy the apps.

These scripts do things like:

- Create projects

- Create service accounts
- Generate SSL certificates
- Deploy apps

This guide includes detailed instructions about how to execute the commands to install the Security Command Center tools using the setup scripts.

Figure 1 provides a high-level overview of the Security Command Center tools, not including the setup scripts:

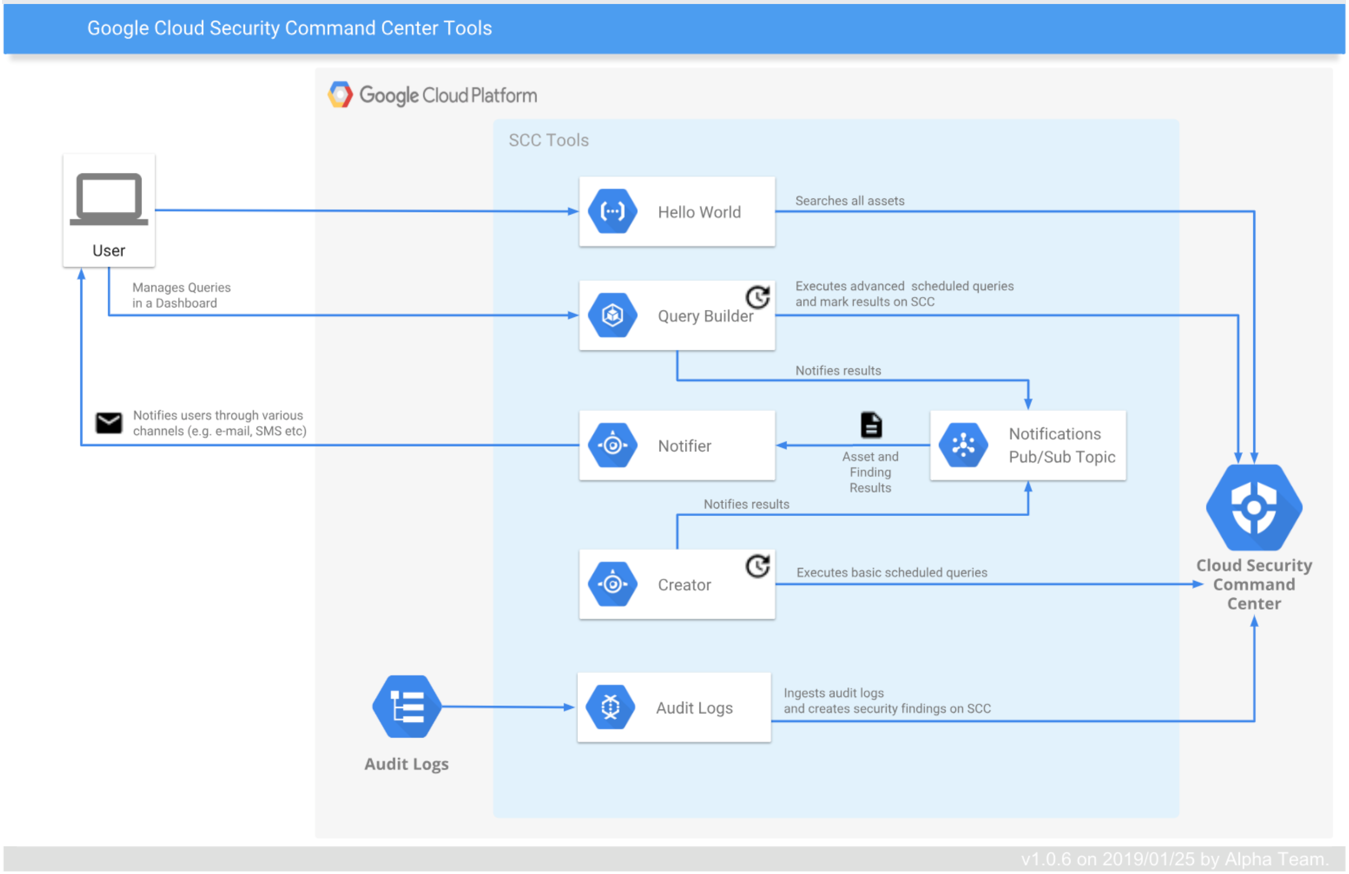
Google Cloud Security Command Center Tools
Google Cloud Platform
SCC Tools
User
Hello World
Searches all assets
Manages Queries in a Dashboard
Query Builder
Executes advanced scheduled queries and mark results on SCC
Notifies results
Notifies users through various channels (e.g. e-mail, SMS etc)
Notifier
Asset and Finding Results
Notifications Pub/Sub Topic
Notifies results
Creator
Executes basic scheduled queries
Cloud Security Command Center
Audit Logs
Audit Logs
Ingests audit logs and creates security findings on SCC
v1.0.6 on 2019/01/25 by Alpha Team.

Figure 1. Diagram of the Security Command Center tools with a description of how each tool interacts with Security Command Center.

To complete this guide, you need the following:

- An active Google Cloud Organization (/resource-manager/docs/organization-setup) with Security Command Center enabled (/security-command-center/docs/quickstart-scc).
- An active Cloud Billing account (/billing/docs/how-to/manage-billing-account).
- The project ID that you want to use to access the Security Command Center API. This project must have the `securitycenter.googleapis.com` API enabled.
- The following Cloud Identity and Access Management roles (/iam/docs/understanding-roles) at the organization level:
  - Billing Account User - `roles/billing.user`
  - DNS Administrator - `roles/dns.admin`
  - Organization Administrator - `roles/resourcemanager.organizationAdmin`
  - Organization Role Administrator - `roles/iam.organizationRoleAdmin`
  - Organization Role Viewer - `roles/iam.organizationRoleViewer`
  - Project Creator - `roles/resourcemanager.projectCreator`
  - Pub/Sub Publisher - `roles/pubsub.publisher`
  - Security Center Admin - `roles/securitycenter.admin`
  - Service Account Admin - `roles/iam.serviceAccountAdmin`
  - Service Account Key Admin - `roles/iam.serviceAccountKeyAdmin`
  - Service Management Administrator - `roles/servicemanagement.admin`

To install the Security Command Center tools, complete the steps below to prepare your environment. After you complete this guide, you can install each tool independently by following the README that's included with the tool.

You must use Cloud Shell to install the tools. Cloud Shell provides command-line access to your Google Cloud resources directly from your browser.

Run the following commands to download the tools package and set up a working directory:

1. Go to the Cloud Console.

   Go to the Cloud Console page (https://console.cloud.google.com/)

2. Click **Activate Cloud Shell**.

3. Get the name of the tools version you want to use. These are stored with a timestamp, so you need to display the Cloud Storage bucket contents.

4. Set environment variables for your working directory and the tools version you want to download.

   a. The Security Command Center tools release version:

   b. The filename for the tools version:

   c. The path for your working directory:

5. Create your working directory:

6. Go to the working directory:

7. Download the Security Command Center tools files by running:

8. Unzip the Security Command Center tools files:

9. Complete setup by following the steps in the README-[VERSION].pdf included in the download.

After you complete the README, you'll be ready to install any of the Security Command Center tools using the tool installation guides.

The tools package you downloaded contains a README that includes installation instructions for each app:

- Hello World: `scc-hello-world-README-$[VERSION].pdf`
- Creator: `scc-creator-README-$[VERSION].pdf`
- Query Builder: `scc-query-builder-README-$[VERSION].pdf`
- Notifier: `scc-notifier-README-$[VERSION].pdf`

- Audit Logs: `scc-audit-logs-README-$[VERSION].pdf`
- Splunk Connector: `scc-connector-README-$[VERSION].pdf`

After you install an app, you can find more information about the app in its user guide:

- Hello World: `scc-hello-world-USER_GUIDE-$[VERSION].pdf`
- Creator: `scc-creator-USER_GUIDE-$[VERSION].pdf`
- Query Builder: `scc-query-builder-USER_GUIDE-$[VERSION].pdf`
- Notifier: `scc-notifier-USER_GUIDE-$[VERSION].pdf`
- Audit Logs: `scc-audit-logs-USER_GUIDE-$[VERSION].pdf`
- Splunk Connector: `scc-connector-USER_GUIDE-$[VERSION].pdf`