# Tenable Cloud Security Quick Reference Guide: Onboarding GCP Accounts in Tenable Cloud Security

Last Revised: May 18, 2023

# Table of Contents

# Onboarding GCP Accounts

This Quick Reference Guide provides the sequence of tasks required to onboard Google Cloud Platform (GCP) cloud accounts to Tenable Cloud Security and to perform a cloud scan. Tenable Cloud Security assesses your cloud infrastructure at runtime to identify security and compliance violations.

## Before you begin:

You must have the following:

- Credentials for your Tenable.io user account.
- A GCP project.

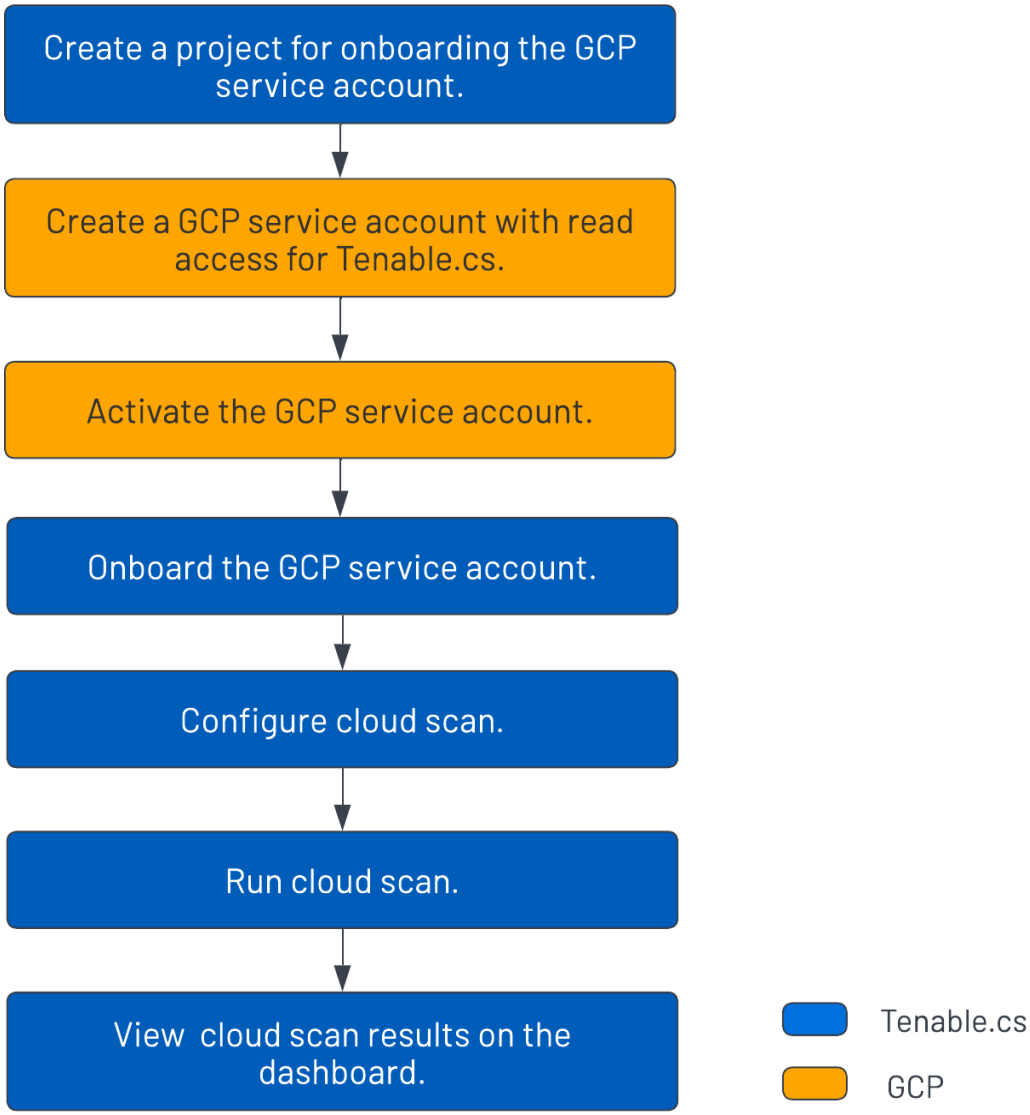
## Overview

You can onboard your Google Cloud Platform (GCP) account by creating a Google service account for Tenable Cloud Security. Service accounts allow applications to authenticate and access Google Cloud resources and services. You must then provide the required permissions to this service account so that Tenable Cloud Security can read the resources in the Google cloud project and scan for vulnerabilities.

After connecting your cloud account, configure your cloud resources and then scan these cloud resources for any violations.

## Workflow

The following workflow provides the high-level tasks required for onboarding GCP accounts.




## Video

**Video:** Onboarding GCP accounts with Tenable.cs

## Other Resources

- Tenable Cloud Security User Guide

  Provides conceptual information and instructions for using Tenable Cloud Security.

- Getting Started with Tenable.cs

  Provides video resources in Tenable Product Education.

# Create a Project

In Tenable Cloud Security Console, you can group resources, such as repositories and cloud accounts, into projects. Projects allow you to monitor, analyze, and manage all your resources at once.

To create a project:

1. Log in to Tenable Vulnerability Management.
2. In the left navigation bar, click **Cloud Security**.

   The Tenable Cloud Security home page appears.
3. In the left navigation bar, click  > **Project**.
4. In the **Give the project a name** section, type a name for your project. For example, **GCP-Project**.
5. Click **Continue**.
6. In the **Choose provider** section, select **Google Cloud** as the cloud service provider.
7. Click **Create**.

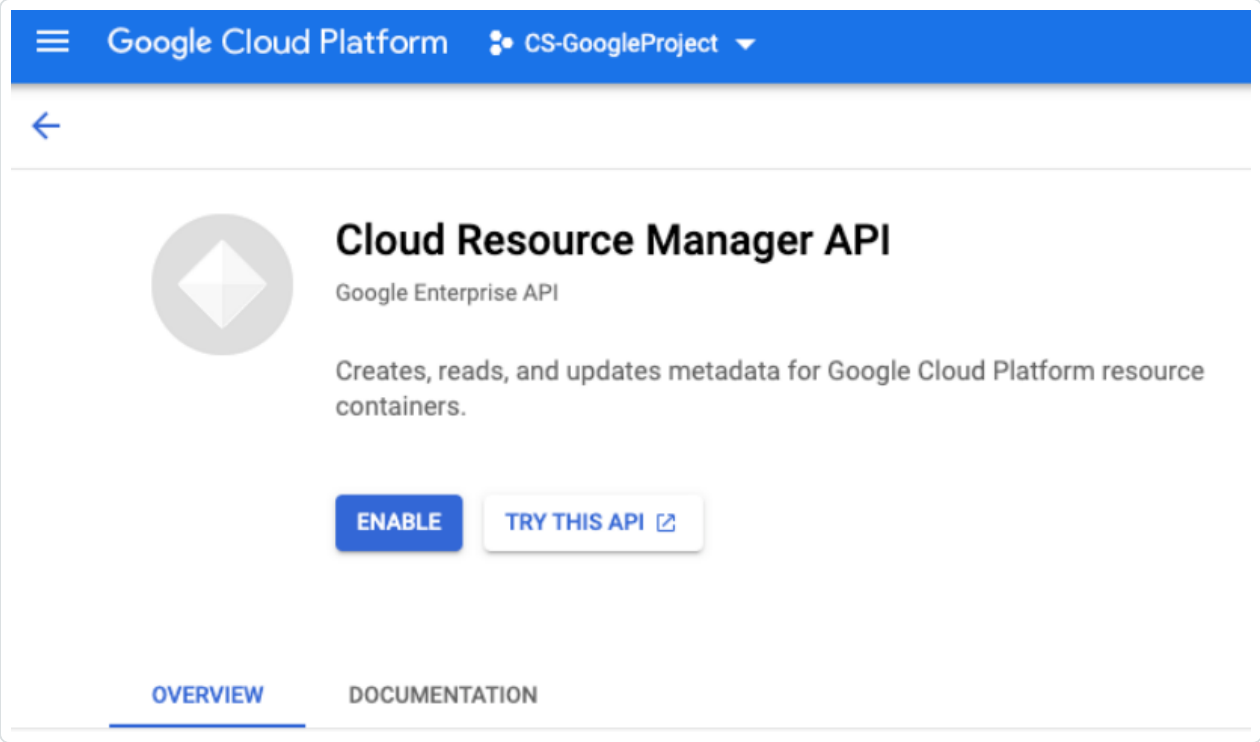
   A confirmation message appears and Tenable Cloud Security creates the project. You can view the new project on the **Projects & Connections** page.

# Create a GCP Service Account

Create a service account for Tenable Cloud Security in Google cloud and then provide read-only access for this service account to your Google cloud project. This provides Tenable Cloud Security with authorized access to the resources in the Google cloud project.

To create a GCP service account:

1. Log in to the Google Cloud console.
2. Select your GCP project from the drop-down box in the top panel.
3. Enable the **Cloud Resource Manager API** service.
    a. Search for **Cloud Resource Manager API** in the search box.
    b. Click **Enable**.




4. On the left navigation bar of the the Google Cloud dashboard, click **IAM & Admin > Service Accounts**.

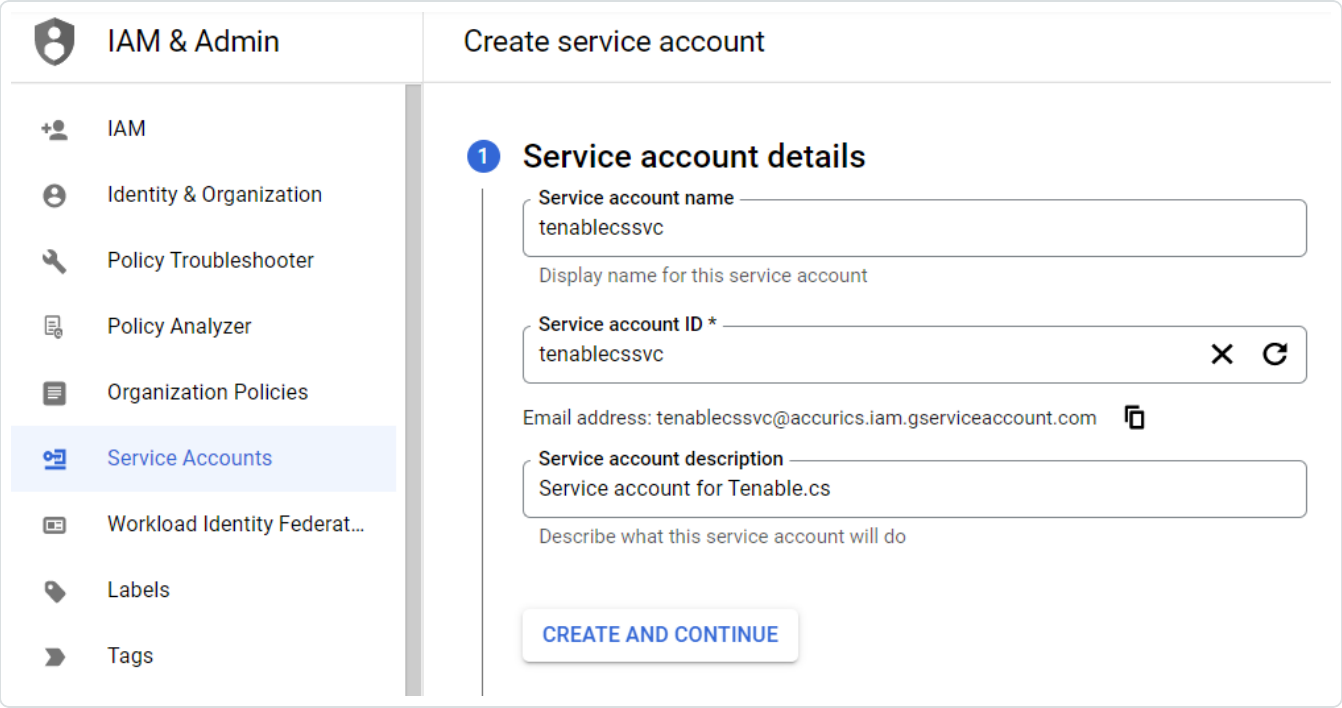
    The **Service accounts** page appears.

5. Click **+ Create Service Account** to create the service account.

The **Create service account** page appears.

6. In the **Service account details** section, provide the following information:

   - **Service account name**: Name of the service account you are creating.
   - **Service account ID**: The **Service account ID** box populates automatically with the name of the service account. The email address of the service account uses this ID. Change the ID, if required.
   - **Service account description**: A description for the service account.

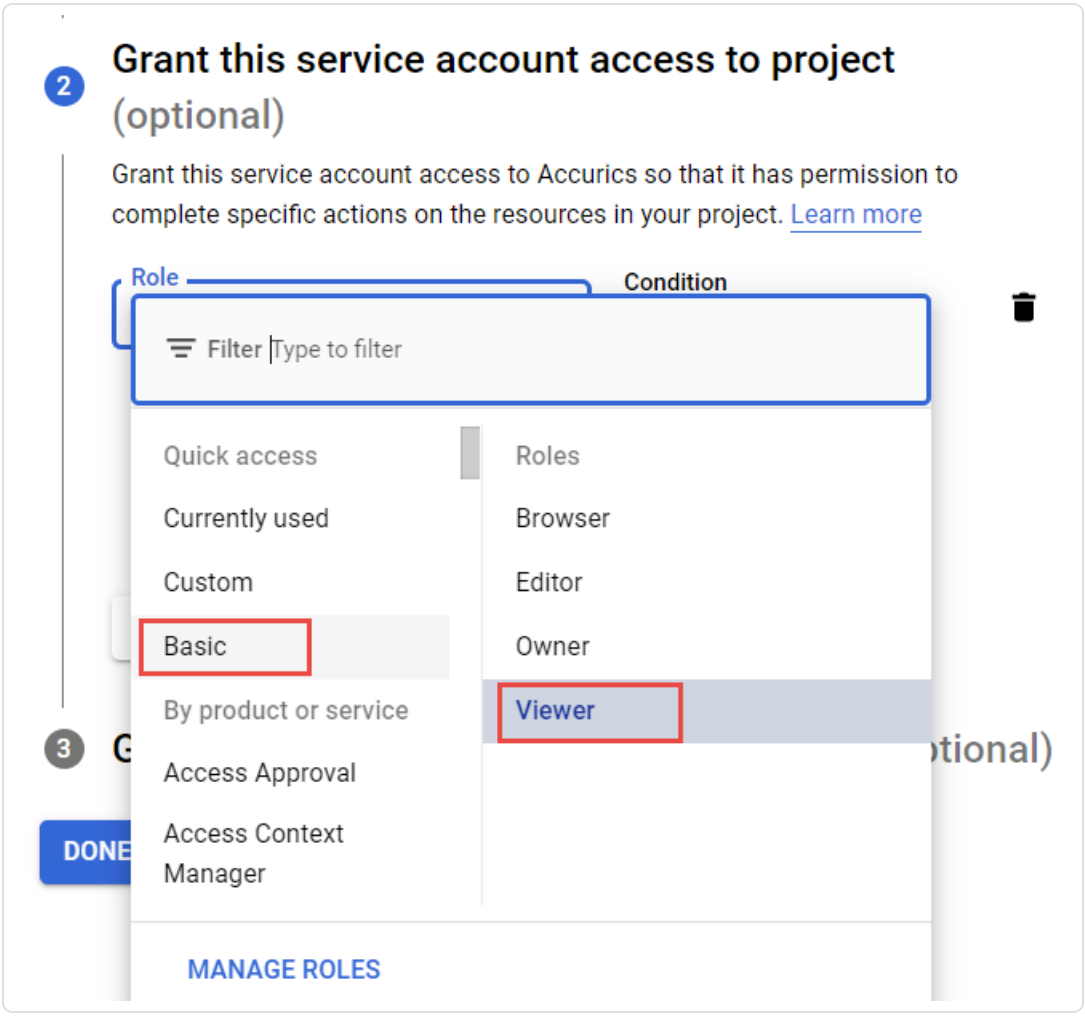



7. Click **Create and Continue**.

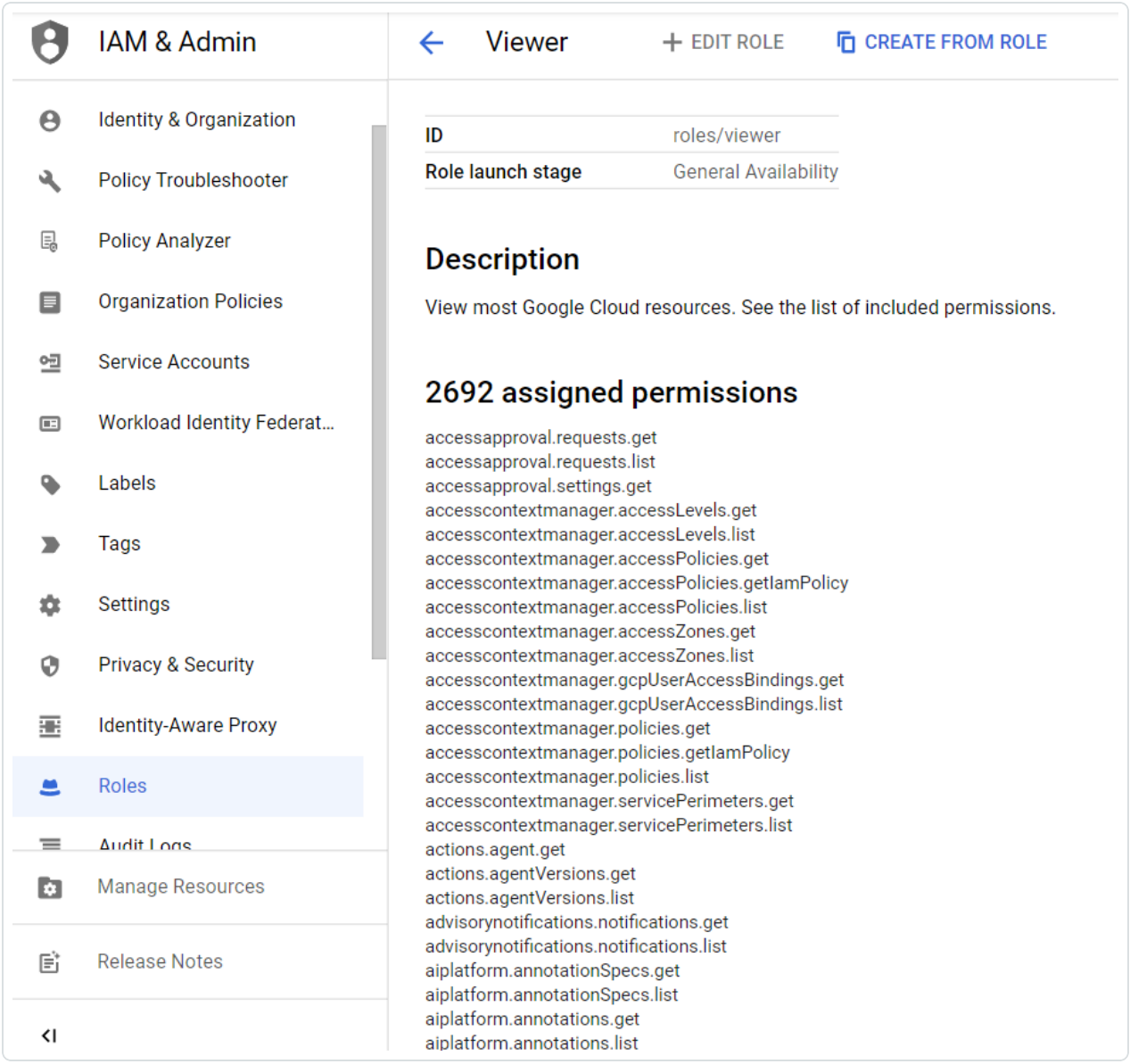
   Google Cloud displays a confirmation message that the service account creation is complete.

8. In the **Grant this service account access to project (optional)** section, provide the service account with access to the GCP project by adding the following role:

- **Viewer**: Click **Basic > Viewer** in the **Role** drop-down box.




This role provides access to Tenable Cloud Security to view most Google Cloud resources. For more information about basic roles, see Basic roles in Google documentation. You can see the list of included permissions for the **Viewer** role from the **Roles** page.



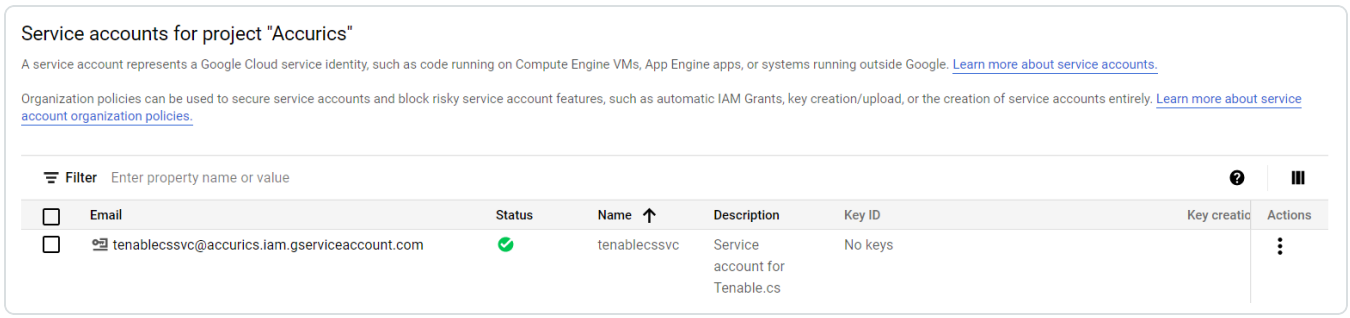

9. Click **Continue**.

   Google Cloud displays a confirmation message that the policy update is complete.

10. (Optional) In the **Grant users access to this service account (optional)** section, add users or groups that need access to this service account.

11. Click **Done**.

    The **Service accounts** page appears with the list of service accounts.

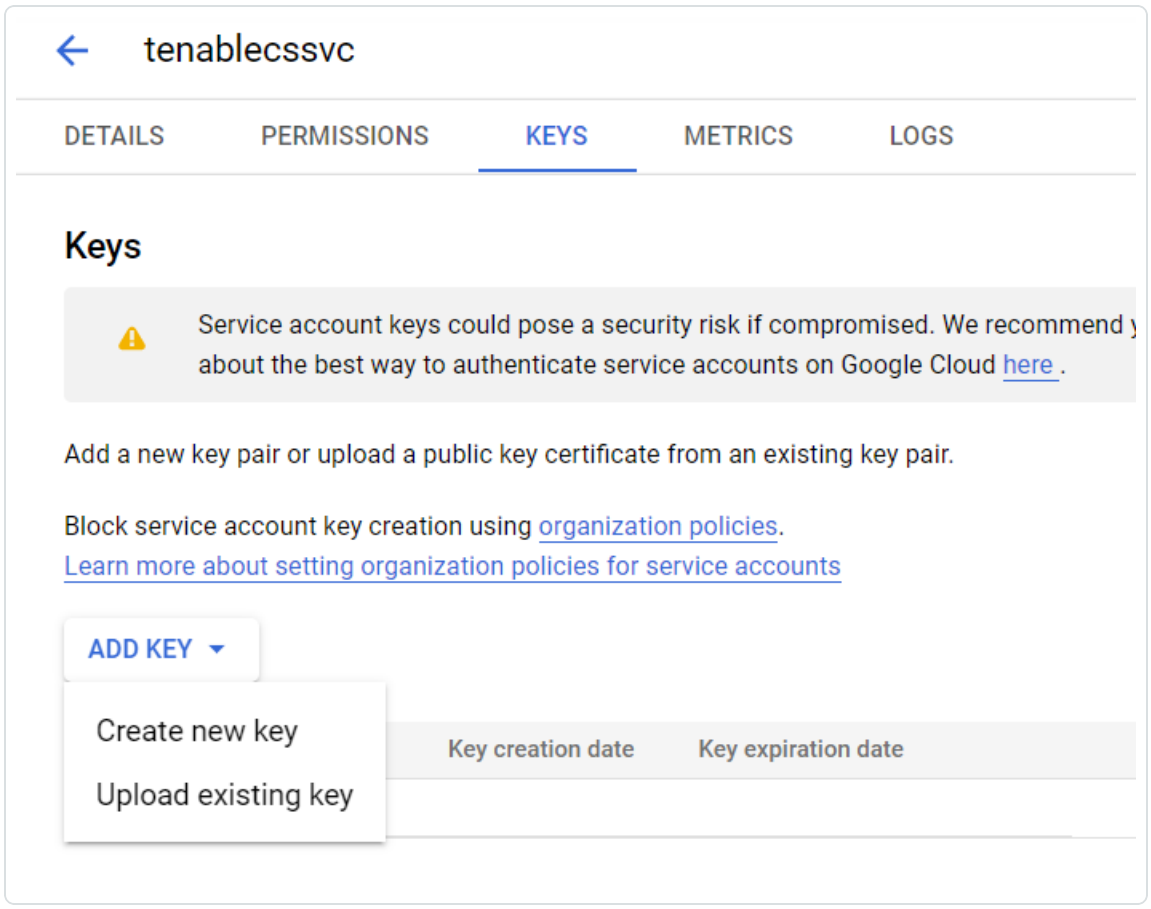



12. Click the service account that you created.

    The **Service account details** page for the service account appears.

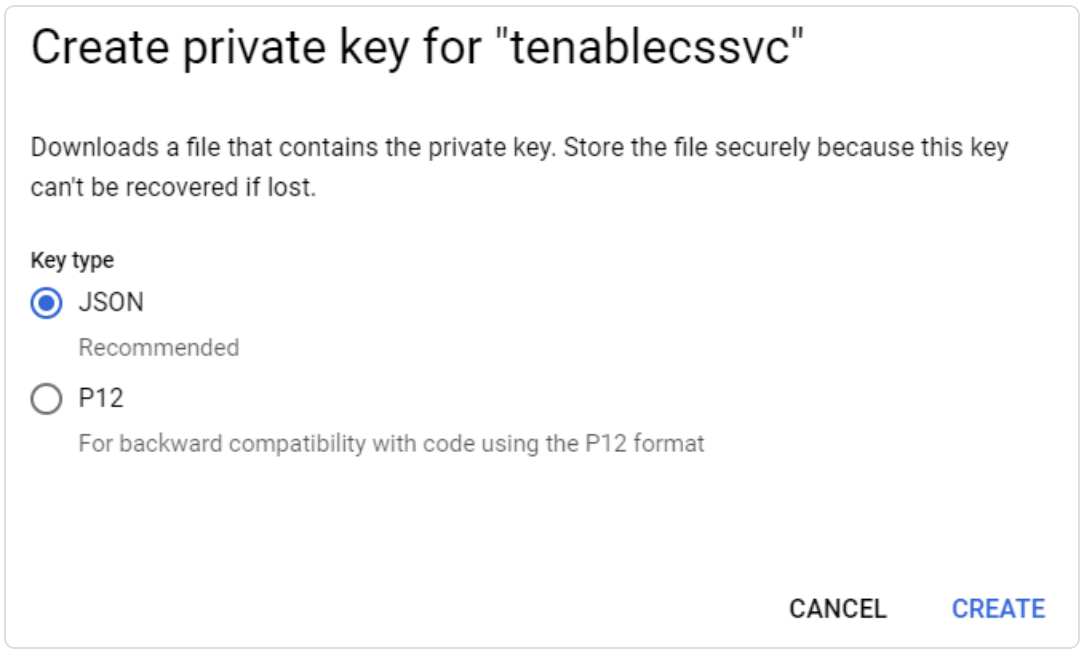
13. Click the **Keys** tab.

    The **Keys** page appears.




14. Click **Add Key > Create new key**.

    The **Create private key** page appears.

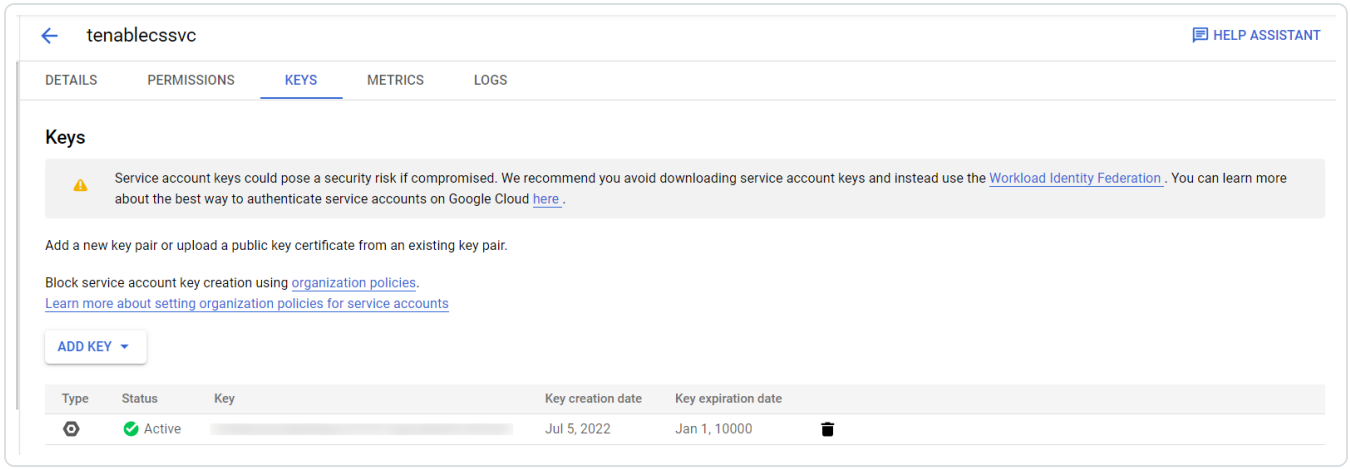



15. In the **Key type** section, select **JSON** and click **Create**.

    A confirmation message appears that the private key JSON file is saved to your computer.

16. Click **Close** to close the confirmation message.

    The new private key and its details appear.




What to do next:

Activate the GCP Service Account.

## Activate the GCP Service Account

After creating the service account for Tenable Cloud Security, you must authorize this service account to access the Google Cloud resources using the Google Cloud CLI. Use the `gcloud auth activate-service-account` command to import the credentials from the JSON file with the private authorization key for the service account and activate it for use.

Before you begin:

- Install the gcloud CLI.

  For more information, see Install the gcloud CLI.

To activate the GCP service account:

1. From the gcloud CLI, run the following command:

   ```
   gcloud auth activate-service-account --key-file=<KEY_FILE>
   ```

   Where:

   - **KEY_FILE** is the path to the JSON key file for the service account. For more information, see Create a GCP Service Account.

   ```
   $ gcloud auth activate-service-account --key-file="C:\tenablecs-0cf0be2a244e.json"
   Activated service account credentials for: [tenablecssvc@tenablecs.iam.gserviceaccount.com]
   ```

2. Verify that you can list the GCP project with the service account credentials:

   ```
   gcloud projects list --sort-by=projectId
   ```

   ```
   $ gcloud projects list --sort-by=projectId
   PROJECT_ID  NAME                PROJECT_NUMBER
   tenablecs   CS-GoogleProject    XXXXXXXXXXXX
   ```

# Activate the GCP Service Account

After creating the service account for Tenable Cloud Security, you must authorize this service account to access the Google Cloud resources using the Google Cloud CLI. Use the `gcloud auth activate-service-account` command to import the credentials from the JSON file with the private authorization key for the service account and activate it for use.

Before you begin:

- Install the gcloud CLI.

  For more information, see Install the gcloud CLI.

To activate the GCP service account:

1. From the gcloud CLI, run the following command:

   ```
   gcloud auth activate-service-account --key-file=<KEY_FILE>
   ```

   Where:

   - **KEY_FILE** is the path to the JSON key file for the service account. For more information, see Create a GCP Service Account.

   ```
   $ gcloud auth activate-service-account --key-file="C:\tenablecs-0cf0be2a244e.json"
   Activated service account credentials for: [tenablecssvc@tenablecs.iam.gserviceaccount.com]
   ```

2. Verify that you can list the GCP project with the service account credentials:

   ```
   gcloud projects list --sort-by=projectId
   ```

   ```
   $ gcloud projects list --sort-by=projectId
   PROJECT_ID  NAME                 PROJECT_NUMBER
   tenablecs   CS-GoogleProject     XXXXXXXXXXXX
   ```

# Onboard a GCP Service Account

You can connect your Google Cloud Platform (GCP) account using a Google service account in Tenable Cloud Security.

Before you begin:

- Make sure you have the private key or GCP credentials file (JSON) for your service account and activated your service account.

  For more information, see Create a GCP Service Account and Activate the GCP Service Account.

To connect to a GCP service account from Tenable Cloud Security:

1. Log in to Tenable.io.
2. In the left navigation bar, click **Cloud Security**.

   The Tenable.cs page opens. By default, a dashboard appears that shows various statistics.
3. In the left navigation bar, click  > **Connection** > **GCP service account**.
4. In the **Choose a workflow to discover GCP service account(s)** section, click **Service account credentials (recommended)**.
5. Click **Continue**.
6. To upload the service account credential file, in the **Discover GCP service account(s)** section, click **Upload** and select the private key JSON file.
7. Click **Continue**.
8. For the discovered account, in the **Choose GCP project(s)** section, do one of the following:
   - To select all available GCP projects, click **All (recommended)**.
   - To select specific projects, click **Specific**, then select a GCP project.

     **Tip:** You can search for a specific project.
9. Click **Continue**.

10. (Optional) In the **Choose projects to add the GCP project(s) to** section, create or select a project for the GCP instance.

    - To create a new project for your GCP account, click **Add a project**. For more information, see Create a Project.
    - Select a project from the list.

11. Click **Connect Cloud Account**.

    You can view the GCP projects linked to the connected GCP account on the **Projects & Connections** page.

# Configure a Cloud Scan

To run a cloud scan after onboarding your cloud accounts, you must select and run a scan profile. Tenable Cloud Security provides a default scan profile for each cloud provider. You can also create your custom scan profiles. After creating a scan profile, you can run a misconfiguration scan for your cloud account. A misconfiguration scan scans for policy violations in IaC repositories and cloud resources. You can view the scan results on the **Findings > Misconfigurations** page.

To configure a cloud scan:

1. Create a Scan Profile.
2. (Optional) Schedule a Scan.

# Create a Scan Profile

Scan profiles allow you to group the scan operations of different cloud resources and schedule scans according to your needs. You can create different scan profiles to run scans targeting different resources.

> **Note:** You can create a maximum of 10 scan profiles.

To create a scan profile:

1. Click **Projects & Connections**.

   Tenable Cloud Security displays the list of projects in the **Projects** tab.

2. In the row for the project for which you are creating the scan profile, click ⋮ **> Manage cloud scan profiles**.

   The **Manage scan profiles** window appears.

3. Click **New Scan Profile**.

   The **Create new scan profile for cloud** window appears.

4. Edit the scan profile name or retain the default name.

5. In **Step 1**, in the **Cloud config assessment options** section, select all applicable resources.

   > **Note:** You can search for resources in the **Search resources** box.

6. Click **Preview** to view the resources selected in the cloud scan profile.

7. Click **Create Scan Profile**.

   Tenable Cloud Security creates the scan profile and displays in the **Manage scan profiles** window.

   For information about how to initiate the scan for the scan profile, see Run a Cloud Scan.

# Schedule a Scan

You can add a scan schedule to your scan profile and run scans at regular intervals.

**Note**: You can add only one schedule for a scan profile.

To schedule a scan for a scan profile:

1. On the home page, click **Projects & Connections**.

   Tenable Cloud Security displays the list of projects in the **Projects** tab.

2. In the row for the project that you want to scan, click ⋮ **> Manage cloud scan profiles**.

   The **Manage scan profiles** window appears.

3. In the row of the scan profile for which you want to schedule a scan, ⋮ **> Schedule scan**.

   The **Schedule scan** window appears.

4. In the **Select interval** drop-down box, select the required schedule to run the scan: Every 6 hours, 12 hours, or 24 hours.

5. Click **Schedule Scan**.

   Tenable Cloud Security schedules the scan for the selected interval and displays a confirmation message.

**Note:** To delete a scheduled scan, in the row for the project, click ⋮ **> Delete scheduled scan**.

# Run a Cloud Scan

You can create a scan profile to include the resource types that you want to scan and trigger a scan for that profile.

To start a scan:

1. Click **Projects & Connections**.

   Tenable Cloud Security displays the list of projects in the **Projects** tab.

2. In the row for the project for the cloud scan, click ⋮ and do one of the following:

   - **Run default scan profile** — Select this option to run a scan on the default scan profile. If there are no other scan profiles, Tenable Cloud Security runs a scan on the system default scan profile.

     > **Note:** Vulnerability scan with agentless assessment is enabled by default for the default scan profile.

   - **Manage cloud scan profiles** — Select this option to create a new scan profile or use a scan profile that you created earlier.

     The **Manage scan profile** window appears and lists all the scan profiles.

   Tenable Cloud Security runs the scan and updates the scan status column of the project on completion of the scan.

What to do next:

After running a cloud scan, you can view a summary of issues, critical security insights, remediation insights, number of cloud and IaC drifts, failing policies, and impacted resources for your project. For more information, see View Tenable Cloud Security Dashboards and Reports.