Tenable.cs Quick Reference Guide: Onboarding GCP Accounts in Tenable.cs

Last Revised: July 15, 2022

Table of Contents

About this Guide

This Quick Reference Guide provides the sequence of tasks required to onboard Google Cloud Platform (GCP) cloud accounts to Tenable.cs and to perform a cloud scan. Tenable.cs 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.

Other Resources

- Tenable.cs User Guide

  Provides conceptual information and instructions for using Tenable.cs.

- Getting Started with Tenable.cs

  Provides video resources in Tenable Product Education.

Onboarding GCP Accounts in Tenable.cs

You can onboard your Google Cloud Platform (GCP) account by creating a Google service account for Tenable.cs. 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.cs 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.

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

Video: Onboarding GCP accounts with Tenable.cs

Create a Project

In Tenable.cs, 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.

Before you begin:

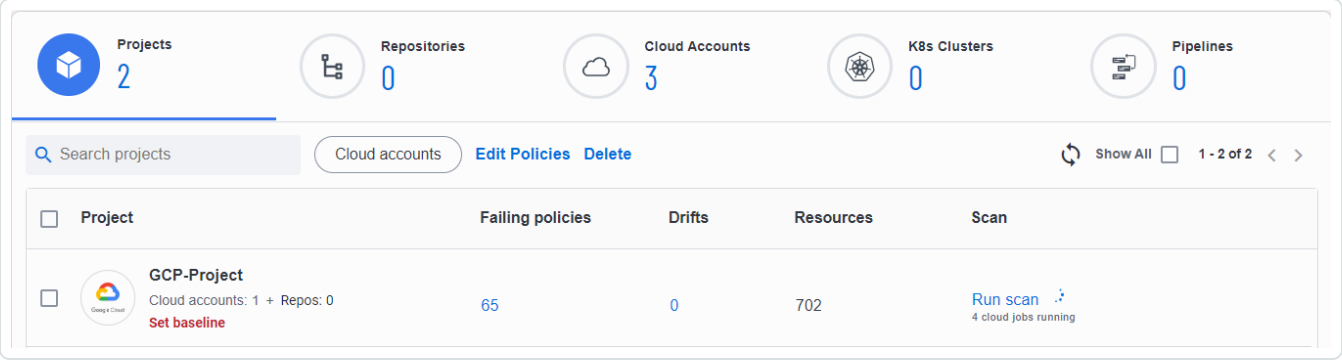
- Obtain credentials for your Tenable.io user account.

To create a project:

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 > **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.cs creates the project. You can view the new project on the **Projects & Connections** page.

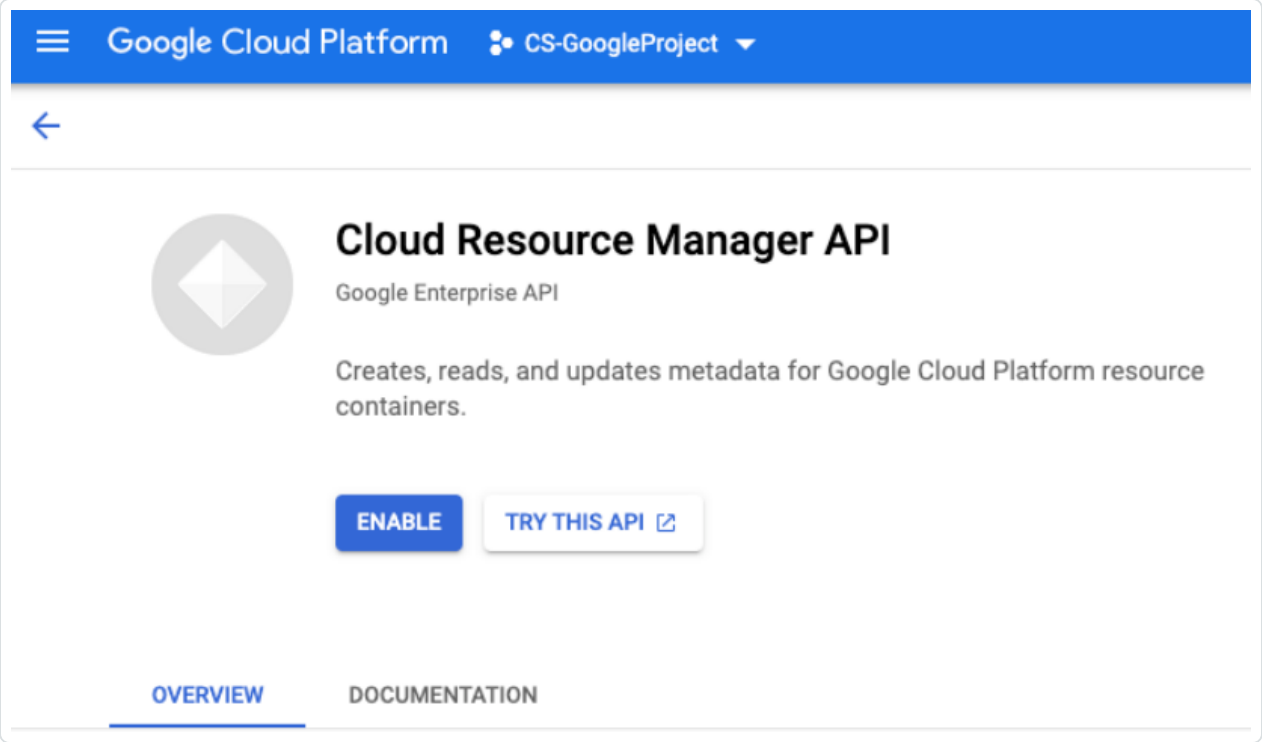


Create a GCP Service Account

Create a service account for Tenable.cs in Google cloud and then provide read-only access for this service account to your Google cloud project. This provides Tenable.cs 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**.

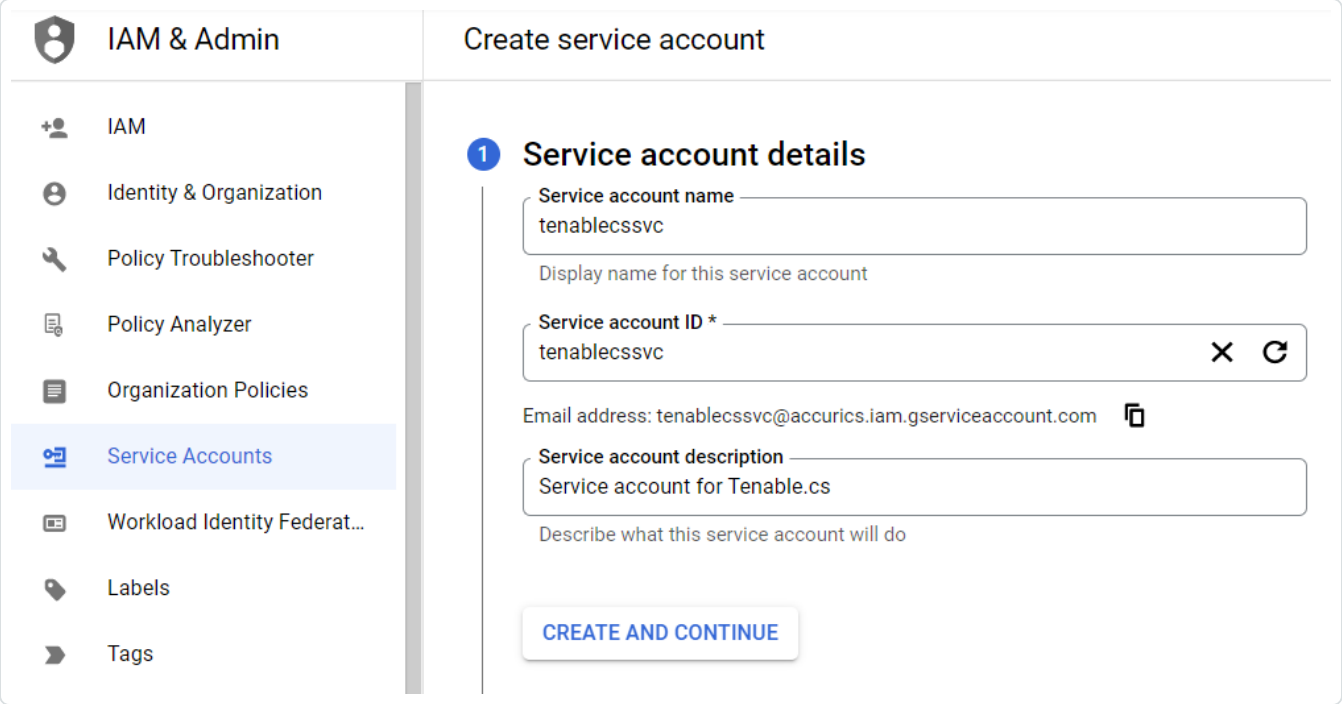
    The **Service accounts** page appears.

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.

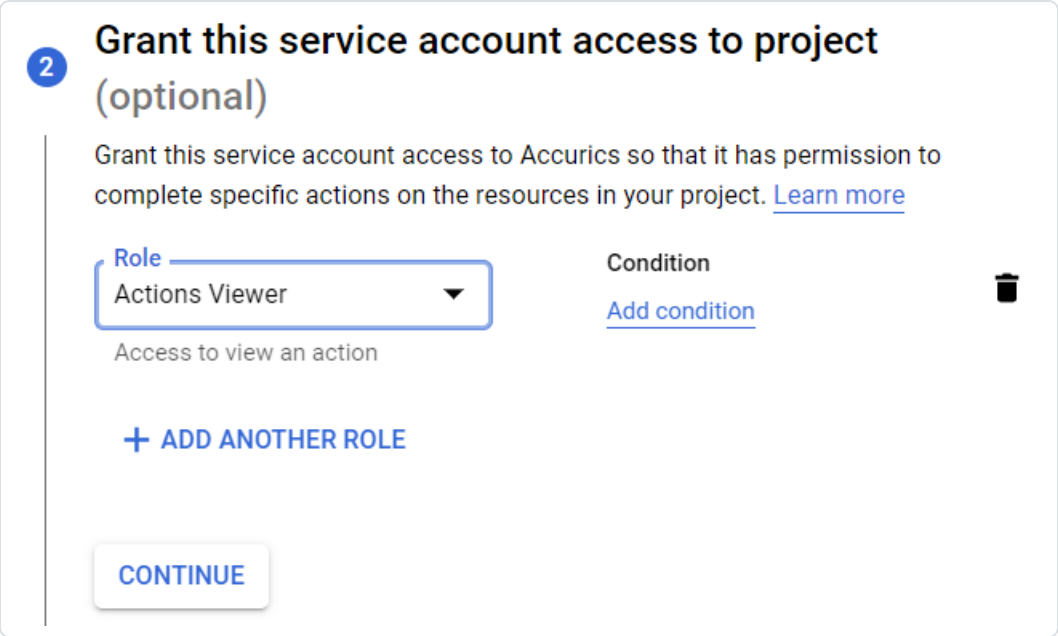


7. Click **Create and Continue**.

   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:

- **Actions Viewer**: Search for **Viewer** in the **Role** drop-down box and select **Actions Viewer**. This role provides the `listClusters` permission to Tenable.cs.



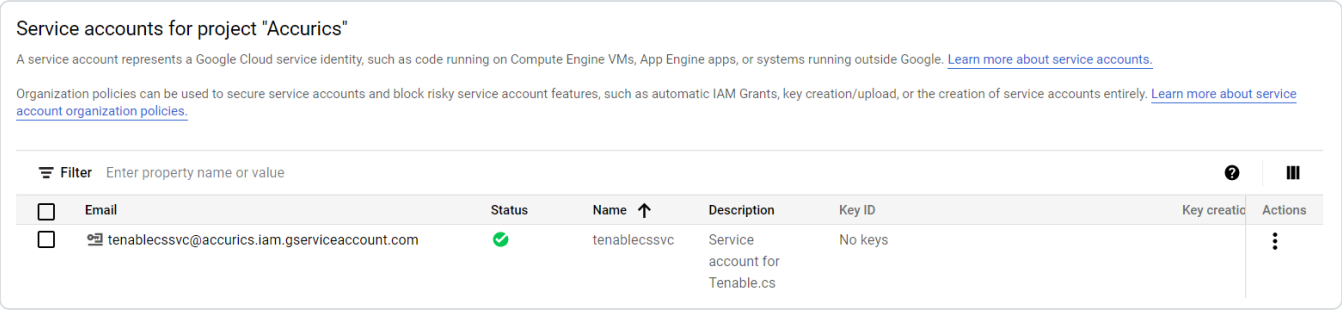
9. Click **Continue**.

   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.

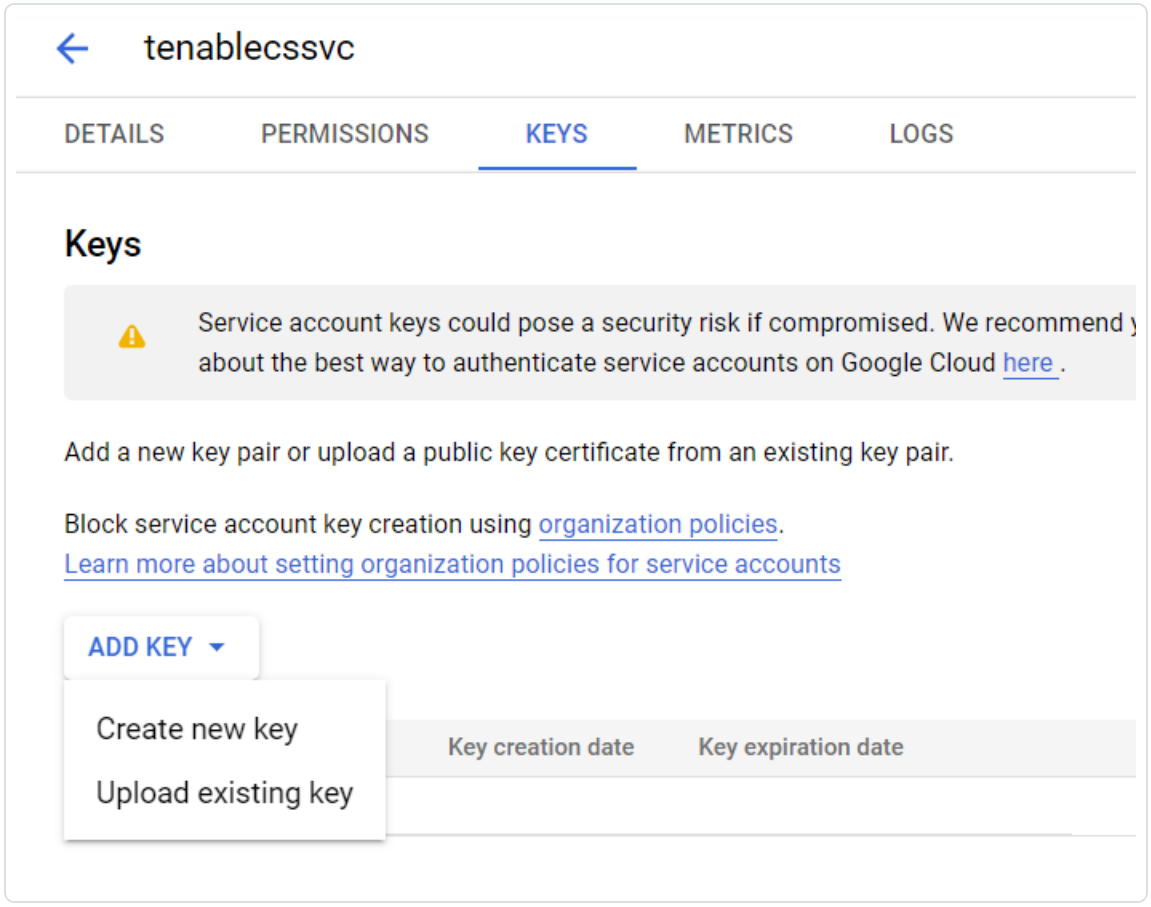


12. Click the service account that you created.

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

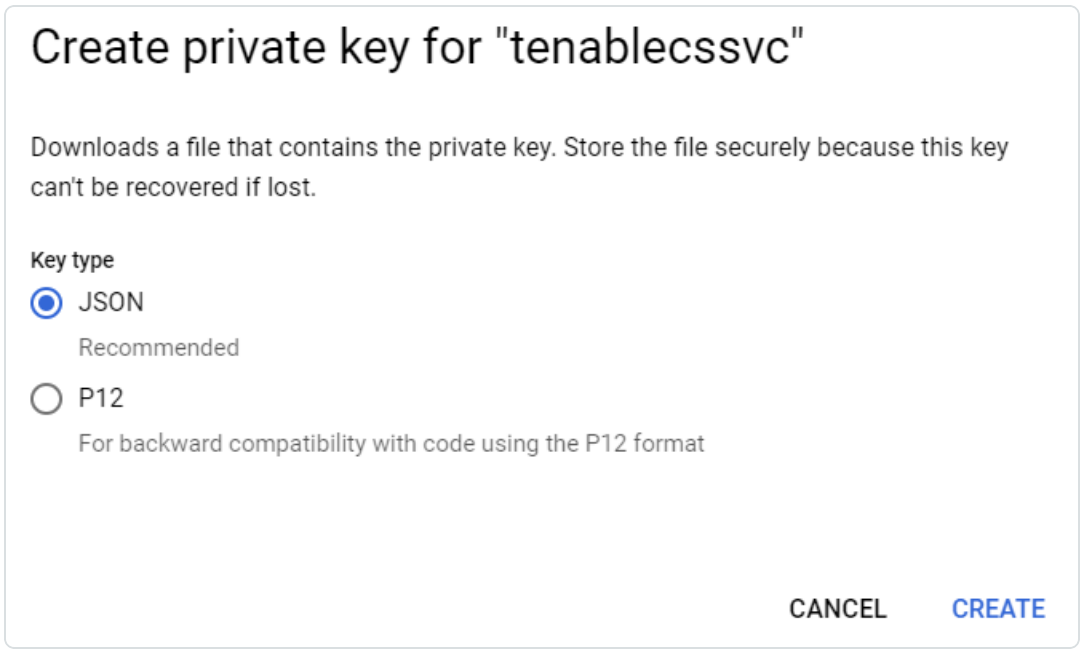
13. Click the **Keys** tab.

    The **Keys** page appears.



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

    The **Create private key** page appears.

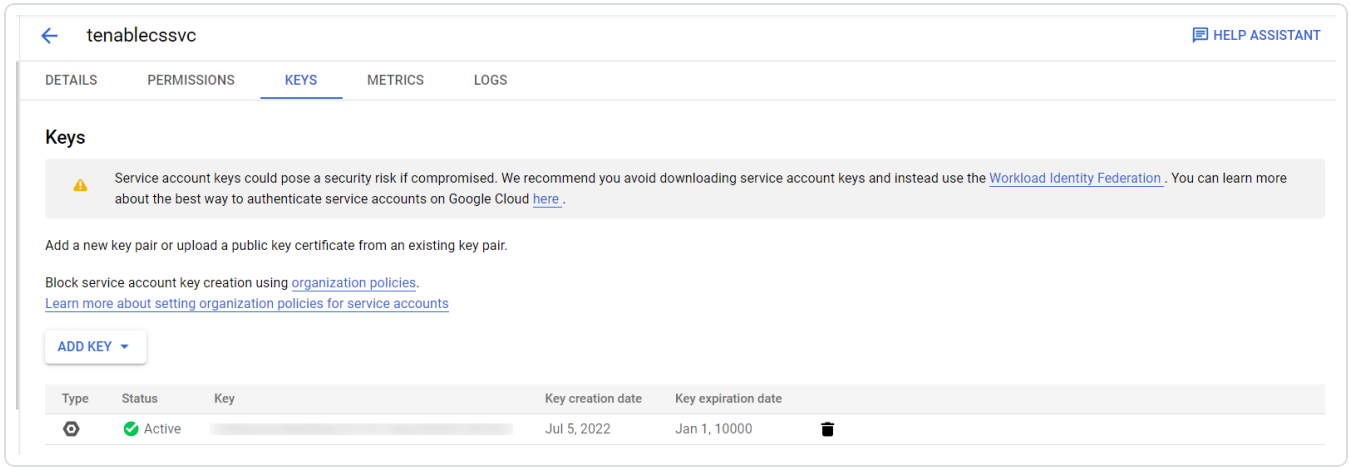


15. In the **Key type** section, select **JSON** and click **Create**.

    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.



Activate the GCP Service Account

After creating the service account for Tenable.cs, 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.cs.

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.cs:

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. In the **Choose type of cloud** section, select **Public cloud**.
7. Click **Continue**.
8. To upload the service account credential file, in the **Discover GCP service account(s)** section, click **Upload** and select the private key JSON file.
9. Click **Continue**.
10. 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.

11. Click **Continue**.
12. (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 Projects.
    - Select a project from the list.
13. Click **Connect Cloud Account**.

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

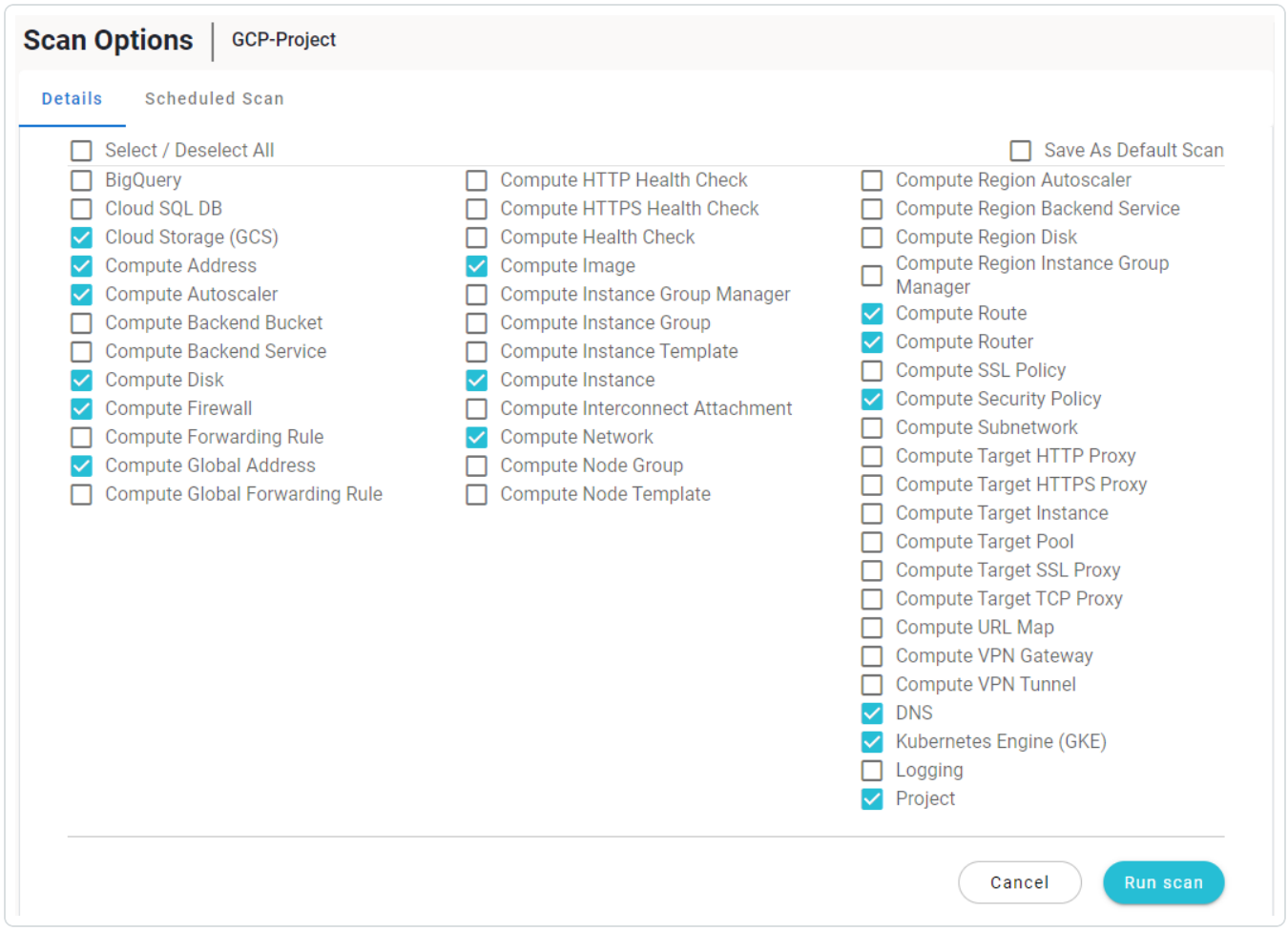
Configure Cloud Scan

After you onboard your cloud accounts, Tenable.cs automatically scans a default set of cloud resources for violations. For subsequent scans, you can configure the cloud resources that you want to scan and set up a scan schedule.

To configure your cloud scan:

1. In the **Scan** column of the project you want to scan, select **Run Scan** > **Configure Cloud Scan**.

   The **Scan Options** window appears.



2. In the **Details** tab, select the types of resources that you want to scan.
3. (Optional) Do any of the following:

- In the upper-right corner, select **Save as Default Scan** to make the selections default.
- In the **Scheduled Scan** tab, create a schedule to run scans at regular intervals (every 6 hours, every 12 hours, every 24 hours).

4. In the **Details** tab, click **Run Scan**.

   A confirmation message appears.

Run Cloud Scan

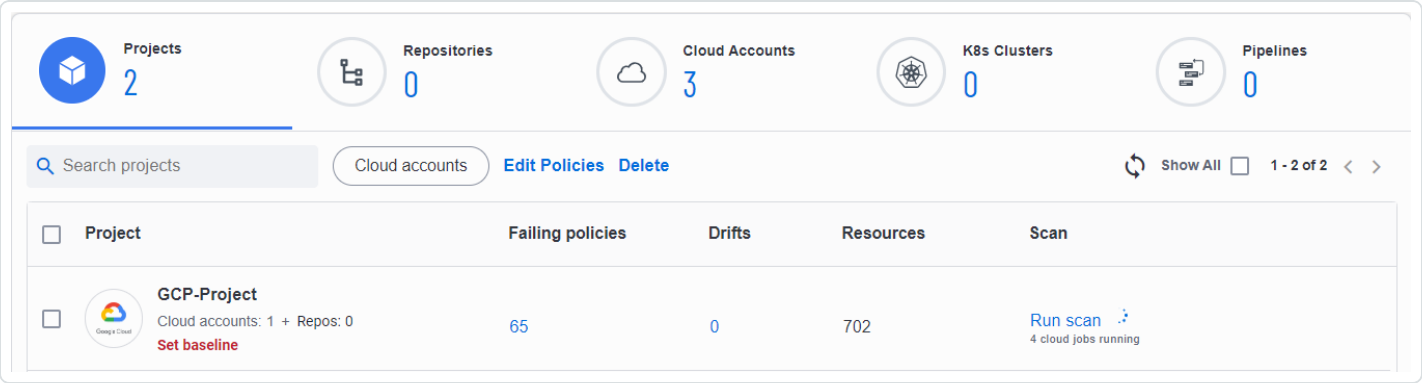
After connecting to your cloud account and configuring your cloud scan, you can scan all the resources in the project for violations.

To start a cloud scan for a project:

1. Go to the **Project and Connection tab**.
2. In the **Scans Column** of the project you want to scan, select **Run scan** > **Cloud Scan**.

   A confirmation message appears and notifies you of any errors during the scan.

Hover over the project to view the number of IaC and cloud resources. When the scan completes, you can view the number of failing policies and drifts for all the resources in the project.



View Results of Cloud Scan

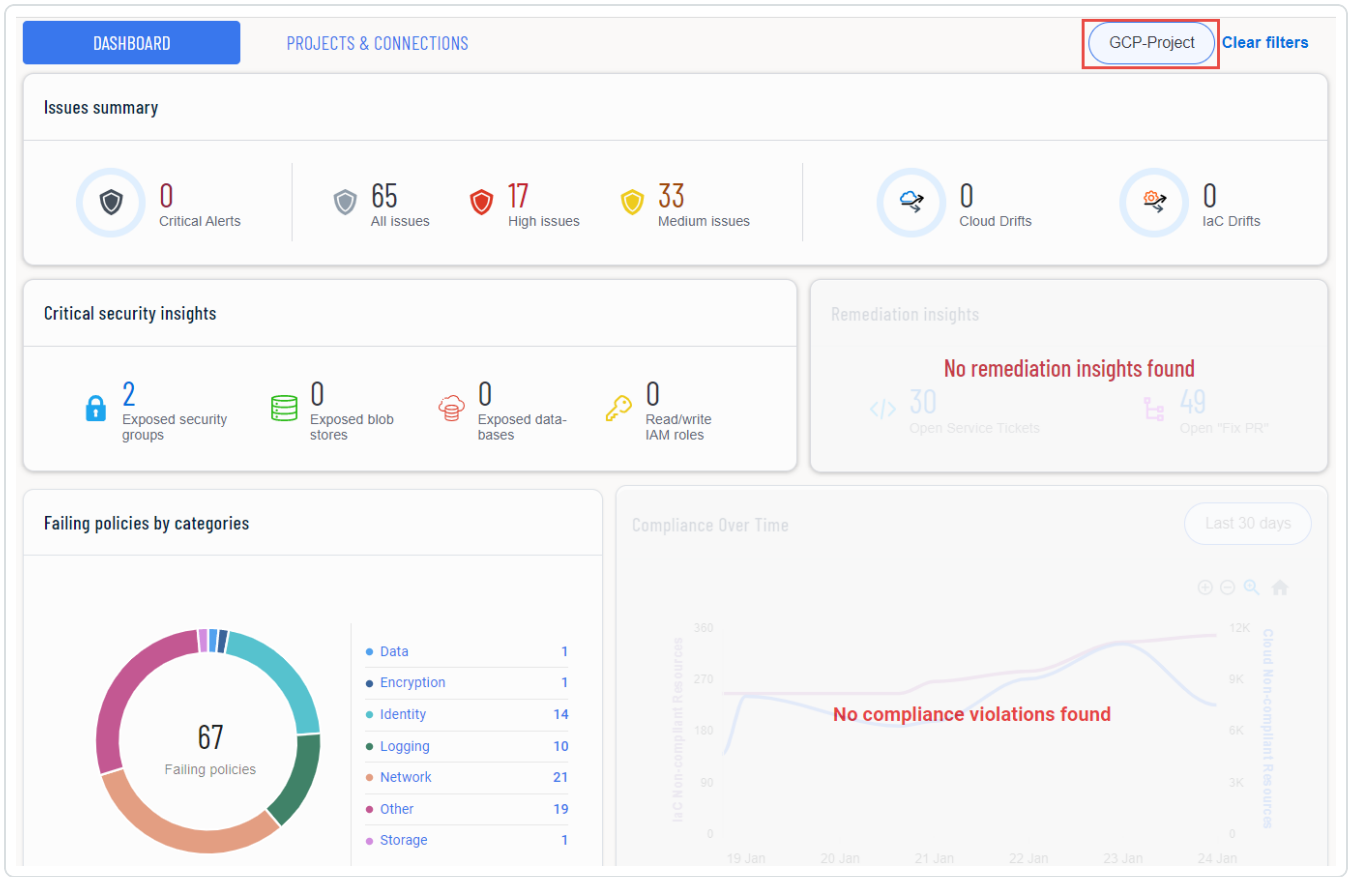
After running a cloud scan, you can view a summary of issues, critical security insights, remediation insights, number of cloud and IaC drifts, failing policies, and impacted resources for your project. The **Projects** tab lists your projects, the number of failing policies on IaC and Cloud, drifts, and the number of resources. You can also view the analytics and statistics of the scan result from the Tenable.cs **Dashboard** page.

To view analytics and statistics for your project:

1. Click **Dashboard**.

   The Tenable.cs dashboard appears that shows the analytical and statistical widgets.

2. To view the summary for your project, in the upper-right corner of the page, click **Projects** and select your project.



3. Click any widget to view its details.

   For a detailed explanation of the widgets on the dashboard, see Tenable.cs Dashboard.

What to do next:

Analyze the failing policies and view the possible remediation in Tenable.cs. For more information, see Analyze Issues and Remediate Issues in Tenable.cs documentation.