



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

---

Last Revised: July 15, 2022



# Table of Contents

<b>About this Guide</b> .....	<b>3</b>
<b>Onboarding GCP Accounts in Tenable.cs</b> .....	<b>4</b>
Create a Project .....	6
Create a GCP Service Account .....	7
Activate the GCP Service Account .....	12
Onboard a GCP Service Account .....	13
Configure Cloud Scan .....	15
Run Cloud Scan .....	17
View Results of Cloud Scan .....	18



## 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](#).

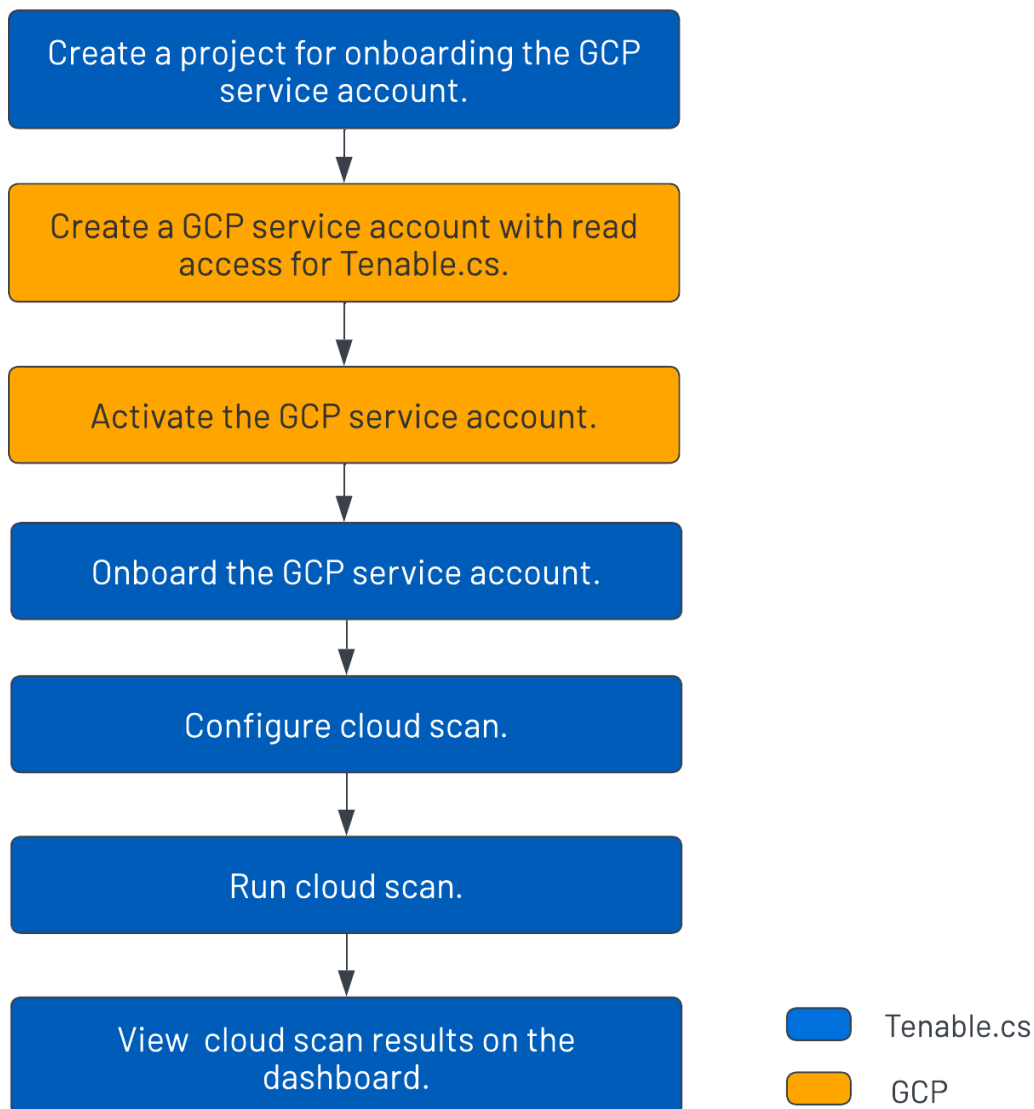


## Onboarding GCP Accounts in Tenable.cs

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.

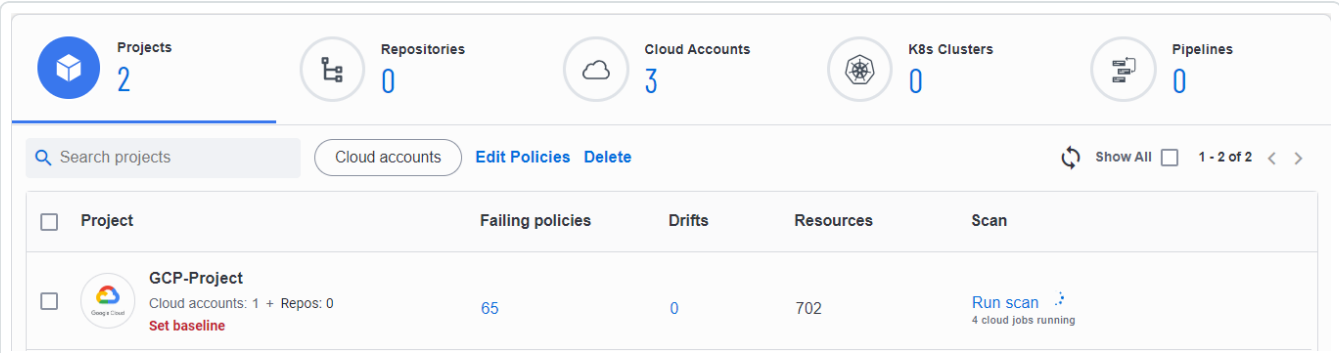
Before you begin:

- 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-Pro-ject**.
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.



The screenshot shows the Tenable dashboard for Projects & Connections. At the top, there are five summary cards: Projects (2), Repositories (0), Cloud Accounts (3), K8s Clusters (0), and Pipelines (0). Below these is a search bar and a filter for 'Cloud accounts'. A table lists the projects, with one project named 'GCP-Project' visible. The table has columns for Project, Failing policies, Drifts, Resources, and Scan. The 'GCP-Project' row shows 65 failing policies, 0 drifts, 702 resources, and a 'Run scan' button with '4 cloud jobs running' below it.

Project	Failing policies	Drifts	Resources	Scan
<input type="checkbox"/>  <b>GCP-Project</b> Cloud accounts: 1 + Repos: 0 <a href="#">Set baseline</a>	65	0	702	<a href="#">Run scan</a>  4 cloud jobs running

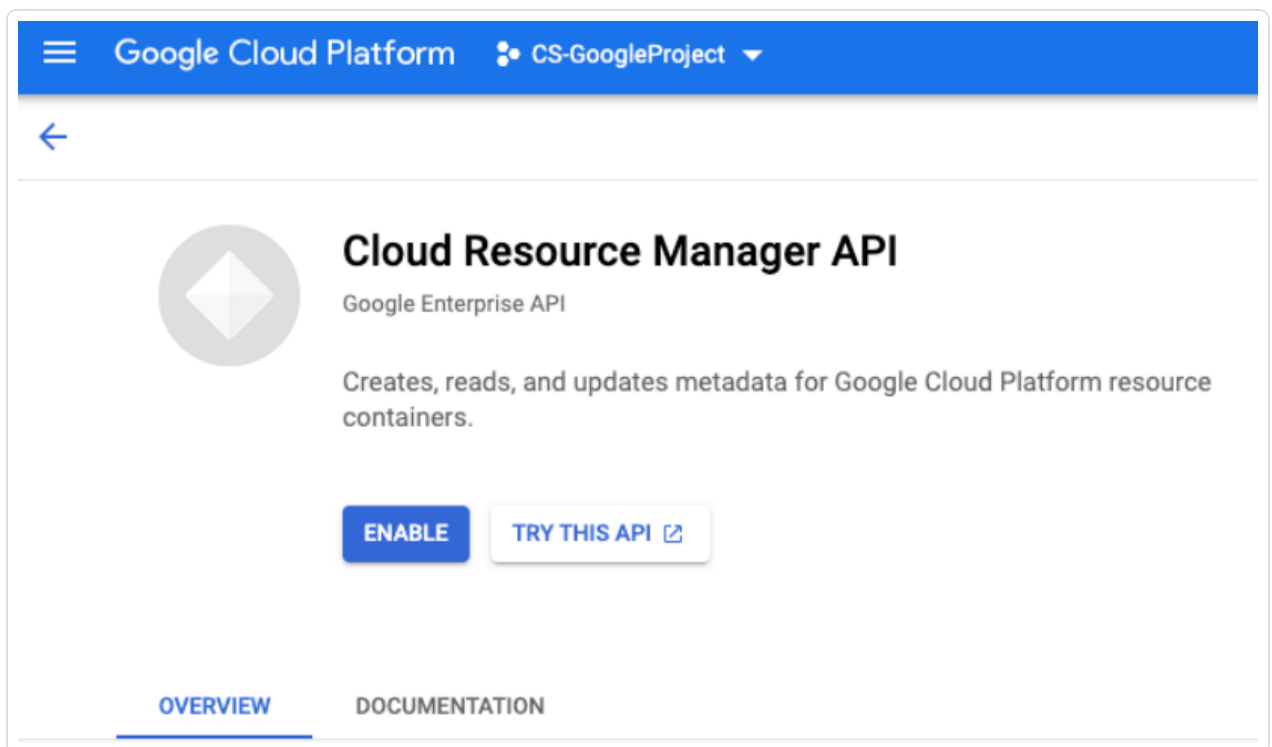


## Create a GCP Service Account

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.

The screenshot shows the Google Cloud IAM & Admin console. The left sidebar is titled 'IAM & Admin' and includes a menu with 'IAM', 'Identity & Organization', 'Policy Troubleshooter', 'Policy Analyzer', 'Organization Policies', 'Service Accounts' (highlighted), 'Workload Identity Federat...', 'Labels', and 'Tags'. The main content area is titled 'Create service account' and features a section labeled '1 Service account details'. This section contains four input fields: 'Service account name' with the value 'tenablecssvc', 'Service account ID \*' with the value 'tenablecssvc', 'Email address' with the value 'tenablecssvc@accurics.iam.gserviceaccount.com', and 'Service account description' with the value 'Service account for Tenable.cs'. Below the fields is a 'CREATE AND CONTINUE' button.

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.

## 2 Grant this service account access to project (optional)

Grant this service account access to Accurics so that it has permission to complete specific actions on the resources in your project. [Learn more](#)

**Role**  **Condition** [Add condition](#)

Access to view an action

[+ ADD ANOTHER ROLE](#)

[CONTINUE](#)

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.

### Service accounts for project "Accurics"

A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or systems running outside Google. [Learn more about service accounts.](#)

Organization policies can be used to secure service accounts and block risky service account features, such as automatic IAM Grants, key creation/upload, or the creation of service accounts entirely. [Learn more about service account organization policies.](#)

**Filter** Enter property name or value ? |||

<input type="checkbox"/>	Email	Status	Name ↑	Description	Key ID	Key creati	Actions
<input type="checkbox"/>	tenablecssvc@accurics.iam.gserviceaccount.com		tenablecssvc	Service account for Tenable.cs	No keys		

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.

The screenshot shows the 'Keys' page for a service account named 'tenablecssvc'. At the top, there is a navigation bar with tabs for 'DETAILS', 'PERMISSIONS', 'KEYS', 'METRICS', and 'LOGS'. The 'KEYS' tab is selected. Below the navigation bar, the page title is 'Keys'. A warning message is displayed: 'Service account keys could pose a security risk if compromised. We recommend you review [Google Cloud documentation](#) about the best way to authenticate service accounts on Google Cloud [here](#).' Below the warning, there is a section with the text: 'Add a new key pair or upload a public key certificate from an existing key pair.' and 'Block service account key creation using [organization policies](#). [Learn more about setting organization policies for service accounts](#)'. At the bottom left, there is an 'ADD KEY' button with a dropdown menu. The dropdown menu is open, showing two options: 'Create new key' and 'Upload existing key'. To the right of the dropdown menu, there is a table with two columns: 'Key creation date' and 'Key expiration date'. The table is currently empty.

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

The **Create private key** page appears.



## Create private key for "tenablecssvc"

Downloads a file that contains the private key. Store the file securely because this key can't be recovered if lost.

### Key type

JSON

Recommended

P12

For backward compatibility with code using the P12 format

CANCEL

CREATE

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.

Type	Status	Key	Key creation date	Key expiration date	
	Active		Jul 5, 2022	Jan 1, 10000	



## 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    XXXXXXXXXXXXX
```



# 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.

**Scan Options** | GCP-Project

**Details** | Scheduled Scan

Select / Deselect All  Save As Default Scan

<input type="checkbox"/> BigQuery	<input type="checkbox"/> Compute HTTP Health Check	<input type="checkbox"/> Compute Region Autoscaler
<input type="checkbox"/> Cloud SQL DB	<input type="checkbox"/> Compute HTTPS Health Check	<input type="checkbox"/> Compute Region Backend Service
<input checked="" type="checkbox"/> Cloud Storage (GCS)	<input type="checkbox"/> Compute Health Check	<input type="checkbox"/> Compute Region Disk
<input checked="" type="checkbox"/> Compute Address	<input checked="" type="checkbox"/> Compute Image	<input type="checkbox"/> Compute Region Instance Group Manager
<input checked="" type="checkbox"/> Compute Autoscaler	<input type="checkbox"/> Compute Instance Group Manager	<input checked="" type="checkbox"/> Compute Route
<input type="checkbox"/> Compute Backend Bucket	<input type="checkbox"/> Compute Instance Group	<input checked="" type="checkbox"/> Compute Router
<input type="checkbox"/> Compute Backend Service	<input type="checkbox"/> Compute Instance Template	<input type="checkbox"/> Compute SSL Policy
<input checked="" type="checkbox"/> Compute Disk	<input checked="" type="checkbox"/> Compute Instance	<input checked="" type="checkbox"/> Compute Security Policy
<input checked="" type="checkbox"/> Compute Firewall	<input type="checkbox"/> Compute Interconnect Attachment	<input type="checkbox"/> Compute Subnetwork
<input type="checkbox"/> Compute Forwarding Rule	<input checked="" type="checkbox"/> Compute Network	<input type="checkbox"/> Compute Target HTTP Proxy
<input checked="" type="checkbox"/> Compute Global Address	<input type="checkbox"/> Compute Node Group	<input type="checkbox"/> Compute Target HTTPS Proxy
<input type="checkbox"/> Compute Global Forwarding Rule	<input type="checkbox"/> Compute Node Template	<input type="checkbox"/> Compute Target Instance
		<input type="checkbox"/> Compute Target Pool
		<input type="checkbox"/> Compute Target SSL Proxy
		<input type="checkbox"/> Compute Target TCP Proxy
		<input type="checkbox"/> Compute URL Map
		<input type="checkbox"/> Compute VPN Gateway
		<input type="checkbox"/> Compute VPN Tunnel
		<input checked="" type="checkbox"/> DNS
		<input checked="" type="checkbox"/> Kubernetes Engine (GKE)
		<input type="checkbox"/> Logging
		<input checked="" type="checkbox"/> Project

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.

The screenshot shows a dashboard with five summary cards: Projects (2), Repositories (0), Cloud Accounts (3), K8s Clusters (0), and Pipelines (0). Below these is a search bar and a filter for 'Cloud accounts'. A table lists projects with columns for Project, Failing policies, Drifts, Resources, and Scan. One project, 'GCP-Project', is shown with 65 failing policies, 0 drifts, and 702 resources. A 'Run scan' button is visible for this project, with a sub-label '4 cloud jobs running'.

Project	Failing policies	Drifts	Resources	Scan
<input type="checkbox"/> GCP-Project Cloud accounts: 1 + Repos: 0 <a href="#">Set baseline</a>	65	0	702	<a href="#">Run scan</a> 4 cloud jobs running



# View Results of Cloud Scan

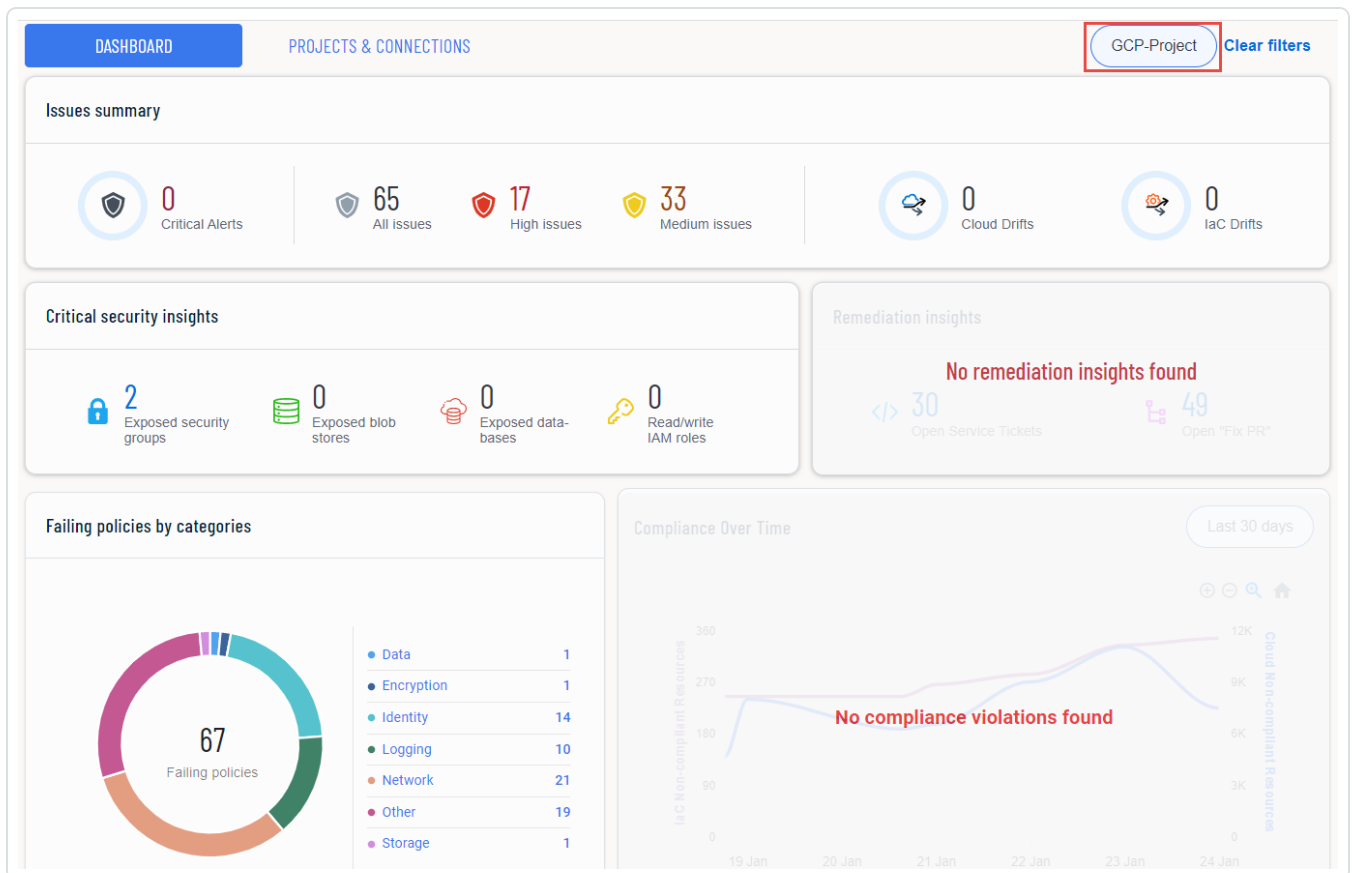
After running a cloud scan, you can view a summary of issues, critical security insights, remediation insights, number of cloud and IaC drifts, failing policies, and impacted resources for your project. The **Projects** tab lists your projects, the number of failing policies on IaC and Cloud, drifts, 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.