



# Tenable and Google Cloud Platform Integration Guide

Last Revised: July 15, 2025



## Table of Contents

<b>Welcome to Tenable for Google Cloud Platform .....</b>	<b>3</b>
<b>Audit Google Cloud Platform .....</b>	<b>4</b>
Configure Google Cloud Platform for a Compliance Audit .....	4
Audit Google Cloud Platform in Tenable Vulnerability Management .....	10
Audit Google Cloud Platform in Tenable Nessus .....	14



---

## Welcome to Tenable for Google Cloud Platform

---

Tenable for Google Cloud Platform (GCP) offers security visibility, auditing, system hardening, and continuous monitoring that allows you to reduce the attack surface and detect malware across your GCP deployments.

Additional benefits of integrating Tenable with GCP include:

- Improved ROI due to the removal of manual verification for misconfigurations on cloud virtual machines
- Reduced security exposure through the prioritization of vulnerable machines and compromised systems

For information about integrating different Tenable products in a GCP environment, see the following:

- [Audit Google Cloud Platform in Tenable Vulnerability Management](#)
- [Audit Google Cloud Platform in Tenable Nessus](#)
- [Google Cloud Platform \(Nessus Compliance Checks\)](#)



---

## Audit Google Cloud Platform

---

To audit Google Cloud Platform (GCP):

1. Configure GCP for use with a compliance audit, as described in [Configure Google Cloud Platform \(Compliance Audit\)](#).
2. Create an audit scan with Tenable Vulnerability Management or Tenable Nessus:
  - [Audit Google Cloud Platform in Tenable Vulnerability Management](#)
  - [Audit Google Cloud Platform in Tenable Nessus](#)

For more information on the Google Cloud Platform audit, see [Google Cloud Platform Audit Compliance Reference](#) in the *Compliance Checks Reference*.

## Configure Google Cloud Platform for a Compliance Audit

To configure Google Cloud Platform (GCP) to support a compliance audit:

Create a new service account to scan Google Cloud Platform.

1. Navigate to **IAM & Admin > Service Accounts**.

The **Service Accounts** page appears.

Google Cloud Platform GCP Nessus Search products and resources

## Create service account

### 1 Service account details

Service account name

Display name for this service account

Service account ID  @gcp-nessus-317015.iam.gserviceaccount.com

Service account description

Describe what this service account will do

CREATE AND CONTINUE

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

### 3 Grant users access to this service account (optional)

DONE CANCEL

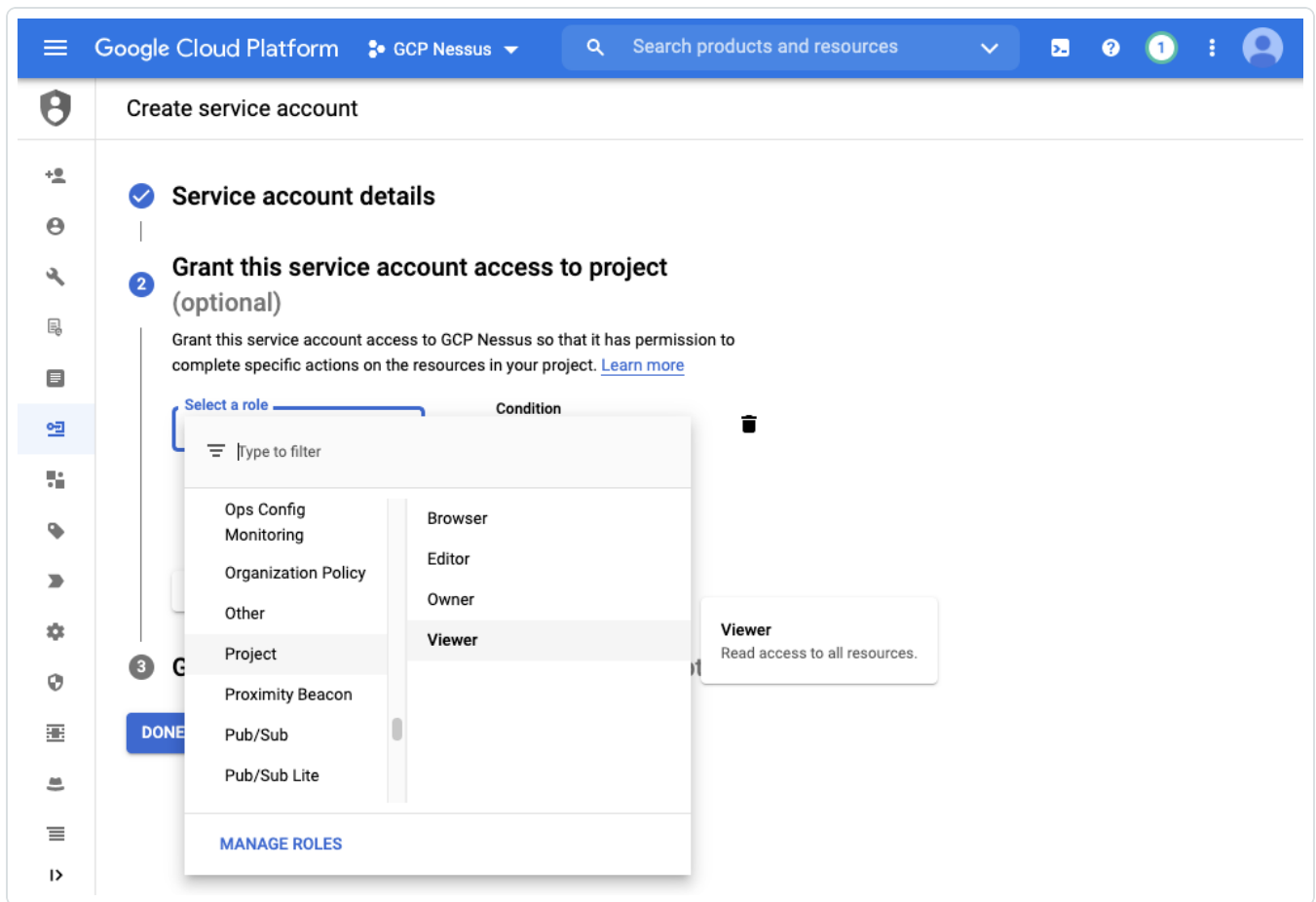
2. Click **Create Service Account**.

The **Create service accounts** page appears.

3. Fill out the **Service account details**.

4. Click **Create and Continue**.

5. In the optional **Grant this service account access to project** section, select **Project>Viewer** in the **Select a role** box.



6. Click **Done**.

The newly created service account appears in a list of available accounts.

Google Cloud PlatformGCP NessusSearch products and resources




Service accounts+ CREATE SERVICE ACCOUNTDELETEMANAGE ACCESS

Service accounts for project "GCP Nessus"

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

	Email	Status	Name ↑	Description	Key ID	Key creation date	Actions
<input type="checkbox"/>	 gcp-nessus@gcp-nessus-317015.iam.gserviceaccount.com		gcp-nessus		No keys		

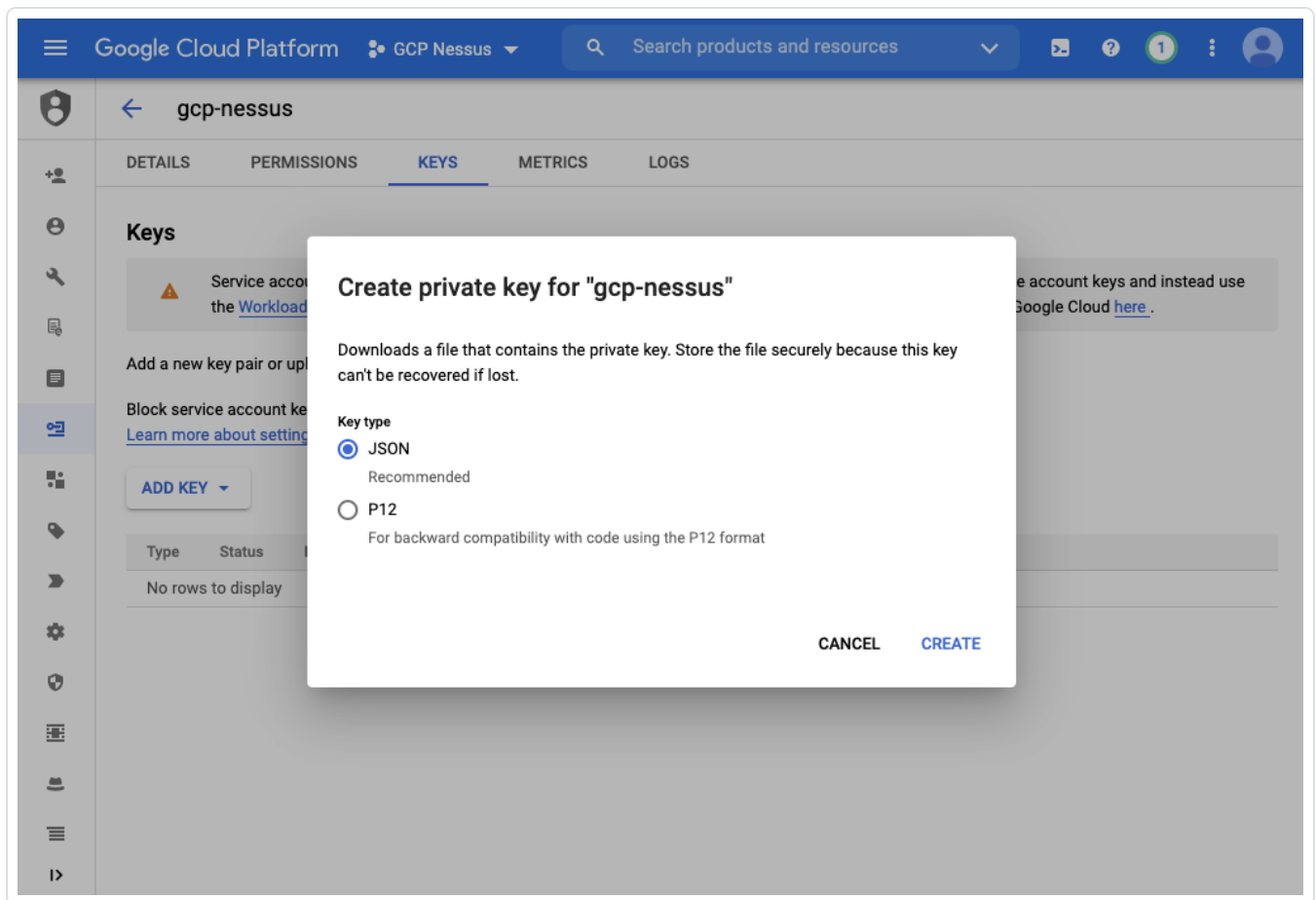
7. Click on the email of the account you just created.

The selected account's page appears.

The screenshot shows the Google Cloud Platform console interface. At the top, the header bar includes the Google Cloud Platform logo, 'GCP Nessus' dropdown, a search bar, and user profile icons. The left sidebar contains navigation icons. The main content area is titled 'gcp-nessus' and has tabs for 'DETAILS', 'PERMISSIONS', 'KEYS' (selected), 'METRICS', and 'LOGS'. Under the 'KEYS' tab, there is a warning message about service account keys, followed by instructions to add a new key pair or upload a public key certificate. Below this, there is a link to 'Block service account key creation using organization policies' and another link to 'Learn more about setting organization policies for service accounts'. An 'ADD KEY' button with a dropdown arrow is present. The dropdown menu is open, showing two options: 'Create new key' and 'Upload existing key'. Below the dropdown, a table is visible with two columns: 'Key creation date' and 'Key expiration date'.

8. In the **Keys** tab, click **Add Key** and select **Create new key** from the drop-down.

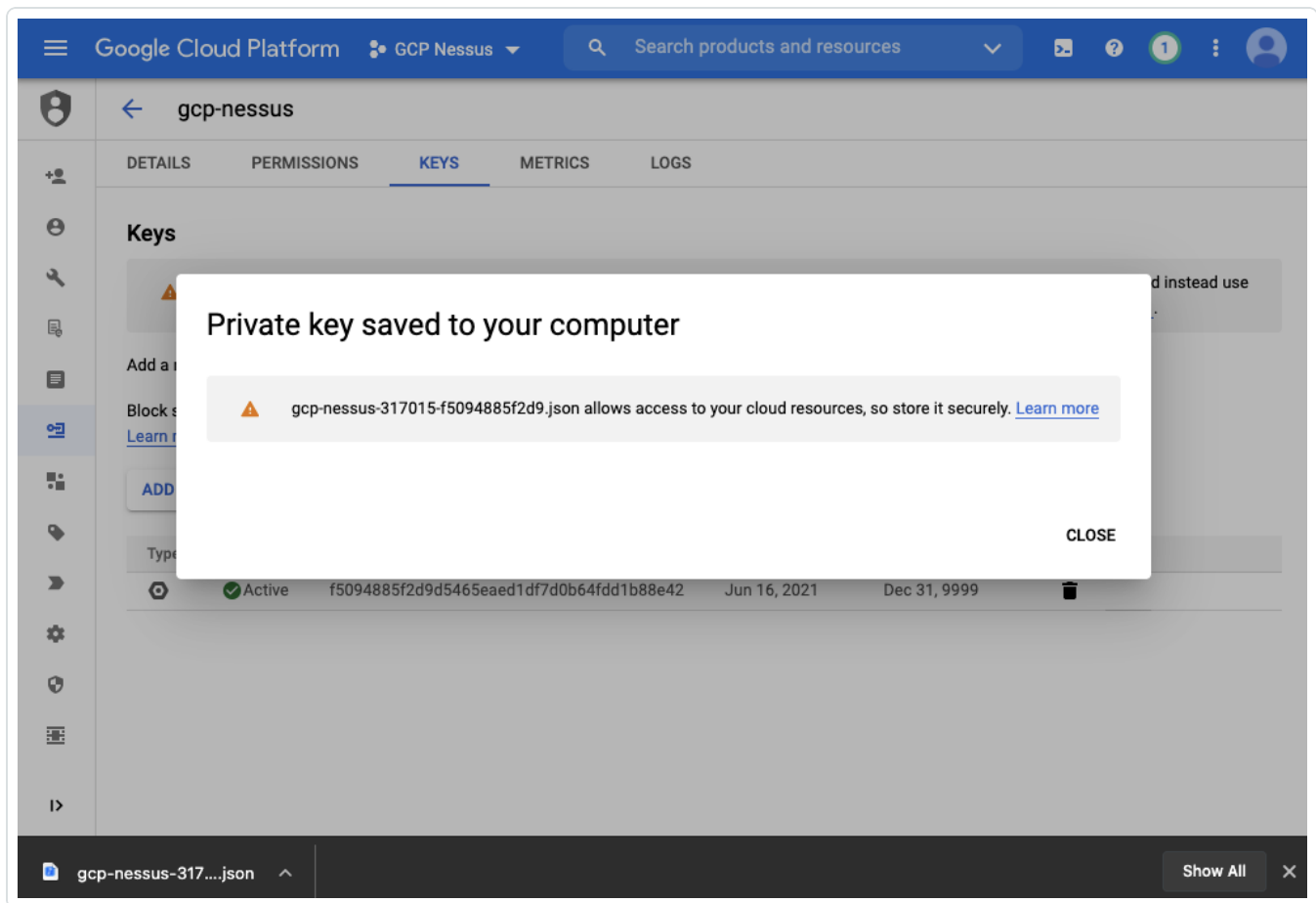
The **Create private key for "your account name"** pop-up appears.



9. Select **JSON** as the key type.

10. Click **Create**.

The **Private key saved to your computer** pop-up appears as confirmation.



11. The **Private key** file will download. This file will be added to the Google Cloud Platform credentials for the scan in Tenable Vulnerability Management or Tenable Nessus.

Repeat these steps for each project you wish to audit or, alternatively, grant the service account access.

What to do next:

Create an audit scan in either Tenable Vulnerability Management or Tenable Nessus:

- [Audit Google Cloud Platform in Tenable Vulnerability Management](#)
- [Audit Google Cloud Platform in Tenable Nessus](#)

## Audit Google Cloud Platform in Tenable Vulnerability Management

Tenable offers the ability to audit the Google Cloud Platform (GCP) environment to detect misconfigurations in the cloud environment and account settings using Tenable Vulnerability Management. Complete the following steps to audit GCP in Tenable Vulnerability Management.



For more information on the GCP audit, see [Google Cloud Platform \(Nessus Compliance Checks\)](#) in the *Compliance Checks Reference*.

Before you begin:

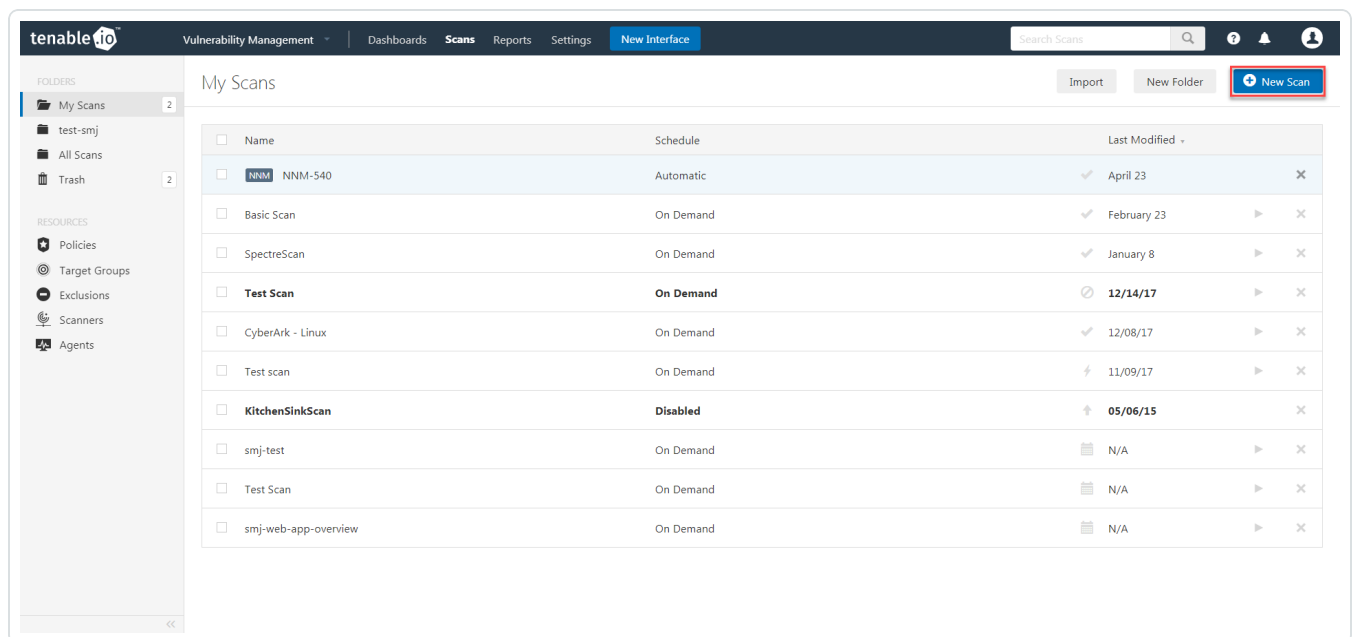
- Configure GCP as described in [Configure Google Cloud Platform for a Compliance Audit](#).

**Note:** No pre-authorization is needed from Google to perform the audit, but a Google Cloud Platform account is required.

To audit GCP in Tenable Vulnerability Management:

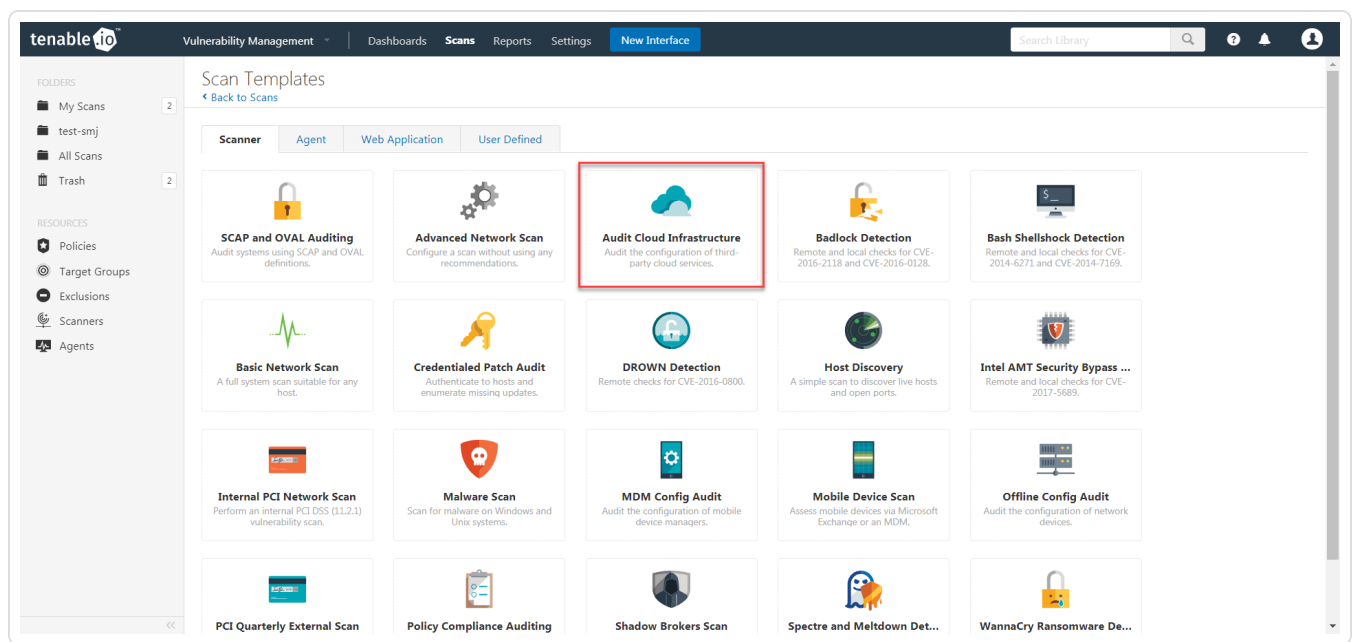
1. Log in to Tenable Vulnerability Management.
2. Click **New Scan**.

The **My Scans** page appears.



3. Select the **Audit Cloud Infrastructure** template.

The **Audit Cloud Infrastructure** page appears.



4. In the **Name** box, type a descriptive name for the scan.
5. (Optional) In the **Description** box, enter information to describe your scan.
6. Click **Compliance**.
7. Click **Google Cloud Platform**.

Tenable offers pre-configured compliance checks and provides the ability to upload a custom GCP audit file.

**Note:** For information on creating a custom audit, see [Google Cloud Platform \(Nessus Compliance Checks\)](#) in the *Nessus Compliance Checks Reference Guide*.

8. Click each compliance check you want to add to the scan.



- If you choose to add a custom audit file, click **Add File** and select the file to upload.

- Click **Credentials**.
- Click **Google Cloud Platform**.
- Click **Add File** and select the JSON key file downloaded during step 11 of [Configure Google Cloud Platform for a Compliance Audit](#).
- Configure the credentials for your selected authentication method.
- Click **Save**.



15. Click the drop-down arrow next to **Save** and select **Launch** to initiate the scan.

**Note:** For additional information on configuring Tenable Vulnerability Management scans, refer to the [Tenable Vulnerability Management User Guide](#).

## Audit Google Cloud Platform in Tenable Nessus

Tenable offers the ability to audit the Google Cloud Platform (GCP) environment to detect misconfigurations in the cloud environment and account settings using Tenable Nessus. Complete the following steps to audit GCP in Tenable Nessus.

For more information on the GCP audit, see [Google Cloud Platform \(Nessus Compliance Checks\)](#) in the *Compliance Checks Reference*.

Before you begin:

- Configure GCP as described in [Configure Google Cloud Platform for a Compliance Audit](#).

**Note:** No pre-authorization is needed from Google to perform the audit, but a Google Cloud Platform account is required.

To audit GCP in Tenable Nessus:



1. Log in to Tenable Nessus.

2. Click **Scans**.

The **My Scans** page appears.

3. Click **+ New Scan**.

The **Scan Templates** page appears.

4. In the **Compliance** section, select the **Audit Cloud Infrastructure** template.

The **Audit Cloud Infrastructure** page **Settings** tab appears.

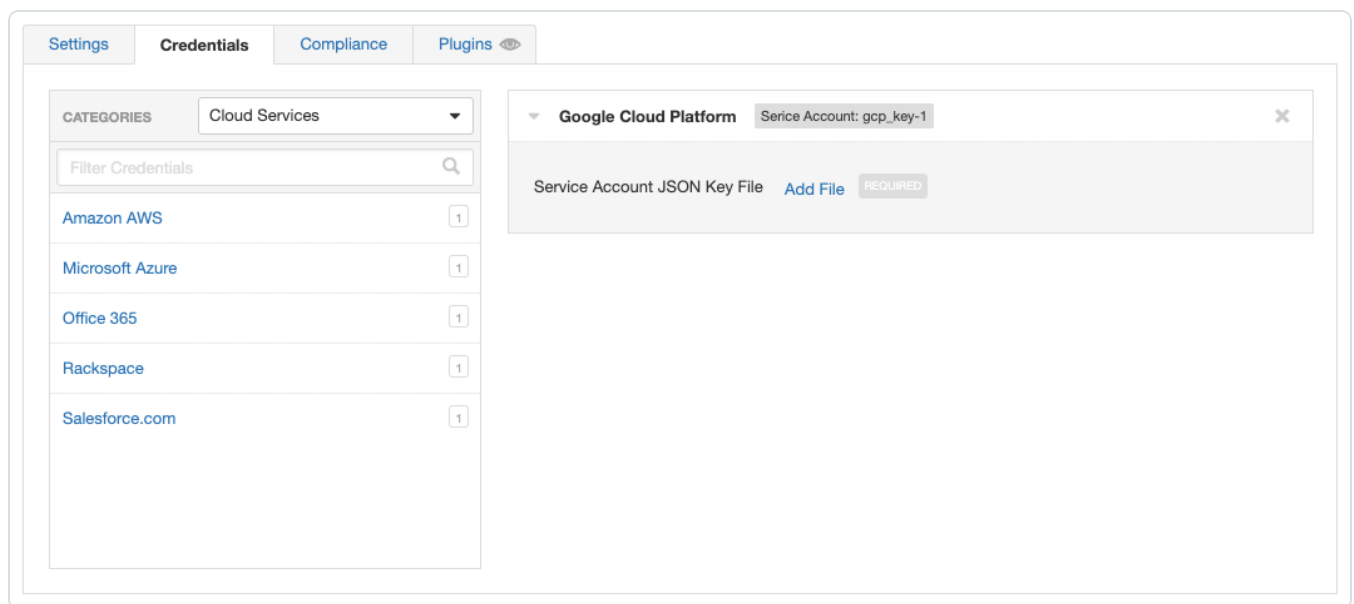
5. In the **Name** box, type a descriptive name for the scan.

6. (Optional) In the **Description** box, enter information to describe your scan.

7. Click the **Credentials** tab.

8. In the **Categories** section, click **Google Cloud Platform**.

The **Google Cloud Platform** options appear.



9. Click **Add File** and select the JSON key file downloaded during step 11 of [Configure Google Cloud Platform for a Compliance Audit](#).

10. Click **Compliance**.

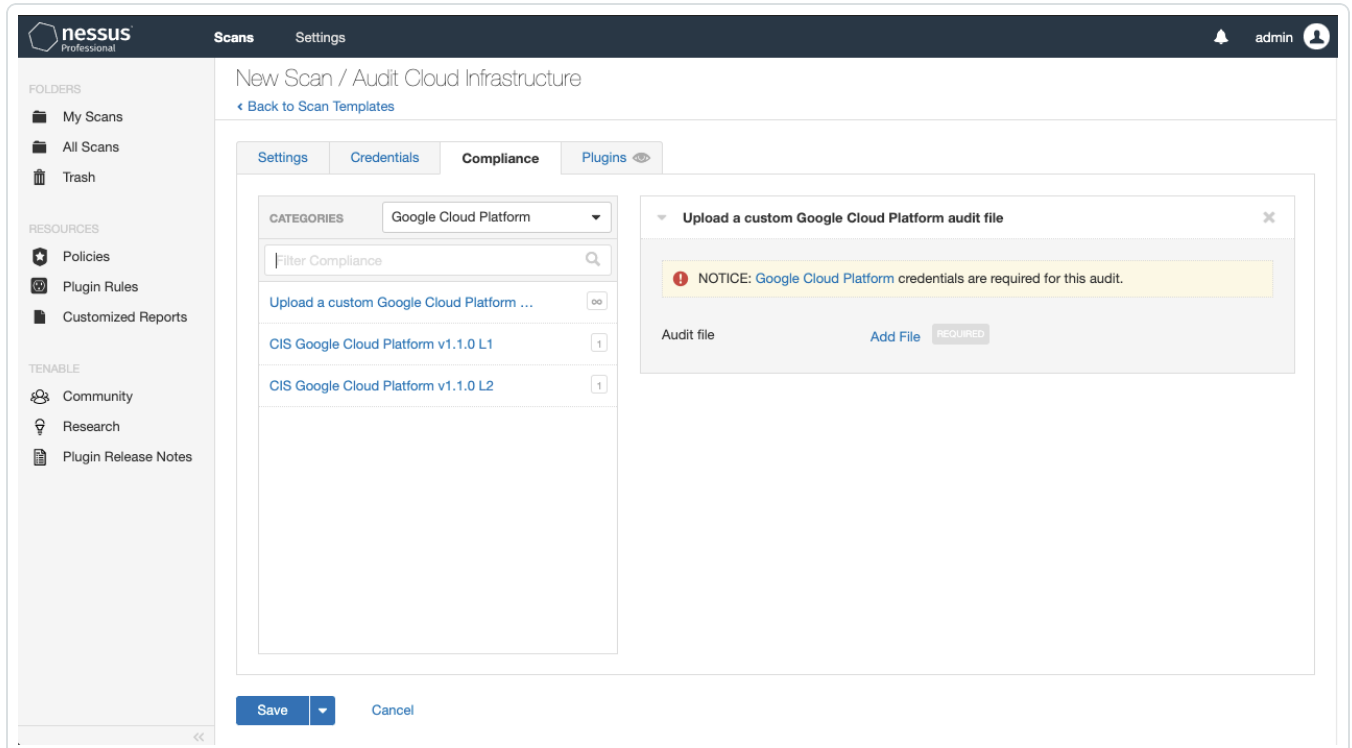
11. Click **Google Cloud Platform**.



Tenable offers pre-configured compliance checks and provides the ability to upload a custom GCP audit file.

**Note:** For information on creating a custom audit, see [Google Cloud Platform \(Nessus Compliance Checks\)](#) in the *Nessus Compliance Checks Reference Guide*.

12. Click each compliance check you want to add to the scan.
13. If you choose to add a custom audit file, click **Add File** and select the file to upload.



14. Click **Save**.

The credential saves and the **My Scans** page appears.

**Note:** For additional information on configuring Nessus scans, refer to the [Tenable Nessus User Guide](#).