Tenable and Google Cloud Platform Integration Guide

Last Revised: December 06, 2021
Table of Contents

Welcome to Tenable for Google Cloud Platform ................................................................. 3

Audit Google Cloud Platform ................................................................................................ 4

Configure Google Cloud Platform for a Compliance Audit ..................................................... 5

Audit Google Cloud Platform in Tenable.io ........................................................................... 11

Audit Google Cloud Platform in Nessus ................................................................................ 15
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.io](#)
- [Audit Google Cloud Platform in 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.io or Nessus:
   - Audit Google Cloud Platform in Tenable.io
   - Audit Google Cloud Platform in 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.

   ![Create service account](image)

   1. Service account details
      - Service account name
        - gcp-nessus
      - Display name for this service account
      - 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)

   4. Click Create Service Account.

The Create service accounts page appears.

2. Fill out the Service account details.

3. 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.
7. Click on the email of the account you just created.

The selected account's page appears.
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.io or 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.io or Nessus:

- [Audit Google Cloud Platform in Tenable.io](#)
- [Audit Google Cloud Platform in Nessus](#)
Audit Google Cloud Platform in Tenable.io

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

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.io:

1. Log in to Tenable.io.
2. Click New Scan.
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)](https://example.com) in the [Nessus Compliance Checks Reference Guide](https://example.com).

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

10. Click **Credentials**.

11. Click **Google Cloud Platform**.

12. Click **Add File** and select the JSON key file downloaded during step 11 of Configure Google Cloud Platform for a Compliance Audit.

13. Configure the credentials for your selected authentication method.

14. Click **Save**.
15. Click the drop-down arrow next to **Save** and select **Launch** to initiate the scan.
Audit Google Cloud Platform in Nessus

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

1. Log in to 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.

![Image of Nessus interface for adding custom audit file]

14. Click Save.

The credential saves and the My Scans page appears.

Note: For additional information on configuring Nessus scans, refer to the Nessus User Guide.