AiVRIC

Getting Started with Google Cloud Platform (GCP)

Overview

This guide provides step-by-step instructions for onboarding a Google Cloud Platform (GCP) environment into AiVRIC.

Onboarding at the **Organization level** enables AiVRIC to securely discover cloud resources, assess risk, and evaluate security posture across all projects under the organization.

AiVRIC uses **least-privilege, read-only access** and follows Google Cloud security best practices.

Prerequisites

Before beginning, ensure you have:

- A **Google Cloud Platform account**
- Access to a **GCP Organization**
- Permissions to:
    - Create service accounts
    - Assign IAM roles at the organization level
- A valid **AiVRIC account**

Supported Scope

AiVRIC supports onboarding at the **Organization level only**.

Organization-level onboarding is required to provide complete visibility and consistent security evaluation across all projects.

High-Level Onboarding Flow

1. Create a service account
2. Assign Viewer permissions at the organization level
3. Generate and download the service account JSON key
4. Capture the GCP Project name
5. Connect GCP to AiVRIC

Step 1: Create a Service Account

AiVRIC uses a dedicated service account to securely access GCP resources.

1. Navigate to **IAM & Admin → Service Accounts**
2. Click **Create Service Account**
3. Provide:
   - **Service account name** (example: aivric-gcp-viewer)
   - **Service account ID** (auto-generated)
   - **Description** (optional)
4. Click **Create and Continue**

Step 2: Assign IAM Role (Viewer)

Assign the **Viewer** role to the service account at the **Organization level**.

1. Navigate to **IAM & Admin → IAM**
2. Switch scope to the **Organization**
3. Click **Grant Access**
4. Add the service account email
5. Assign the role:
   - **Viewer** (roles/viewer)
6. Save changes

This role provides read-only access required for discovery and assessment.

Step 3: Generate Service Account JSON Key

1. Go to **IAM & Admin → Service Accounts**
2. Select the newly created service account
3. Open the **Keys** tab
4. Click **Add Key → Create New Key**
5. Select **JSON**
6. Click **Create**

A JSON key file will be downloaded to your system.
Store this file securely — it will be used to authenticate with AiVRIC.

Step 4: Capture the GCP Project Name

AiVRIC requires the **Project Name** to associate discovered resources.

To capture the project name:

1. Open **Google Cloud Console**
2. Select a project from the project selector (top navigation)
3. Navigate to **IAM & Admin → Settings**
   or **Project Info**
4. Copy the value labeled **Project name**

⚠️ Note: Use the **Project Name**, not the Project ID.

Step 5: Connect GCP to AiVRIC

1. Log in to the **AiVRIC Platform**
2. Navigate to **Integrations / Cloud Accounts**
3. Select **Google Cloud Platform**
4. Paste the **Service Account JSON key contents**
5. Paste the **GCP Project Name**
6. Submit the integration

AiVRIC will validate the credentials and begin organization-level discovery.

Data Access & Security

- Access is **read-only**
- No configuration or production resources are modified
- Credentials are encrypted at rest and in transit
- Access can be revoked at any time by removing the service account or role

---

Post-Onboarding Validation

Once onboarding is complete, confirm the following in AiVRIC:

- GCP organization and projects are visible
- Cloud resources appear in inventory
- Security findings begin populating
- Compliance and risk assessments are initialized

Discovery time may vary based on environment size.

Updating or Revoking Access

Rotate Credentials

- Generate a new JSON key for the service account
- Paste the new key in AiVRIC
- Delete the old key from GCP

Revoke Access

- Remove the Viewer role from the service account
  or
- Delete the service account entirely

Support

For onboarding issues or questions:

- Contact **AiVRIC Support**
- Validate permissions with your GCP Organization administrator