IRON FORT

Granting IronFort Access to Your Google Cloud Environment

What Is This?

IronFort is a compliance and security platform that reviews your Google Cloud environment for vulnerabilities, misconfigurations, and compliance gaps.

To perform this work, IronFort needs read-only access to your Google Cloud project(s) for:

- Automated scanning performed by an IronFort-managed Google Cloud service account
- Manual compliance review performed by IronFort compliance specialists through a managed Google Group

Both access paths are read-only. IronFort can view your cloud configuration and security posture, but cannot make changes to your environment.

How IronFort Accesses Your Account

IronFort uses these two identities:

- Service account for automated scanning: `ext-compliance-ops@external-identities-475520.iam.gserviceaccount.com`
- Google Group for compliance review: `ironfort-complianceops-external@goironfort.com`

You will grant the same read-only roles to both identities.

Before You Start

What You Will Need

- Access to the Google Cloud Console
- The **Owner**, **IAM Admin**, or equivalent permission to manage IAM on the Google Cloud project(s) you want to connect
- Permission to enable APIs on the project, if they are not already enabled

Required APIs

Make sure these APIs are enabled on each Google Cloud project you want IronFort to review:

- `Service Usage API`
- `Identity and Access Management (IAM) API`

Step-by-Step Setup Instructions

Step 1 - Open Your Google Cloud Project

1. Go to https://console.cloud.google.com.
2. In the top navigation bar, select the project you want to connect to IronFort.

Step 2 - Enable the Required APIs

1. In the left-hand menu, go to **APIs & Services**.
2. Select **Library**.
3. Search for `Service Usage API` and click **Enable** if it is not already enabled.
4. Return to the API Library.
5. Search for `Identity and Access Management (IAM) API` and click **Enable** if it is not already enabled.

> **Note:** You only need to enable these APIs once per project. If you see a button for `Manage` that means these APIs are already enabled.

Step 3 - Go to IAM

1. In the left-hand menu, click **IAM & Admin**.
2. Select **IAM**.

Step 4 - Grant Access to Both IronFort Identities

Repeat these steps for each of the following identities:

- `ext-compliance-ops@external-identities-475520.iam.gserviceaccount.com`
- `ironfort-complianceops-external@goironfort.com`

For each identity:

1. Click the **+ Grant Access** button near the top of the page.
2. In the **New principals** field, enter the email address.

Step 5 - Assign the Required Read-Only Roles

For each identity, add the following roles:

1. `Viewer` under **Basic**
2. `Service Usage Consumer` (`roles/serviceusage.serviceUsageConsumer`) under **Service Usage**
3. `Security Reviewer` under **IAM**
4. `Cloud Asset Viewer` under **Cloud Assets**
5. `Security Center Admin Viewer` under **Security Center**

Then click **Save**.

> **Note:** These roles are read-only. They allow IronFort to review your resources, configuration, and relevant Google security findings without making changes.

Step 6 - Confirm Access

After saving, both IronFort identities should appear in your IAM list. Confirm that each identity has the required roles.

Let your IronFort contact know you have completed these steps, and they will confirm the connection and begin your first scan.

Why IronFort Requests Both Access Paths

IronFort uses two identities because automated scanning and manual compliance review serve different purposes.

The service account supports automated scans. The Google Group supports manual review by authorized IronFort compliance specialists. Together, they allow IronFort to assess your environment more completely while keeping access read-only.

This supports reviews against frameworks such as:

- **HIPAA** - Health Insurance Portability and Accountability Act
- **SOC 2** - System and Organization Controls 2
- **ISO 27001** - International information security standard
- **ITSG-33** - IT Security Guidance for the Government of Canada
- **NIST** - National Institute of Standards and Technology Cybersecurity Framework

---

Frequently Asked Questions

Can IronFort make changes to my environment? No. The roles listed above are read-only. IronFort cannot create, modify, or delete resources in your environment.

What data does IronFort collect? IronFort reads resource configurations such as firewall rules, storage settings, IAM policies, and Google security findings to identify security and compliance issues. No application data or sensitive customer data is accessed.

Can I revoke access? Yes. At any time, return to **IAM & Admin > IAM** and remove either or both of the IronFort identities.

Who is in the IronFort compliance group? `ironfort-complianceops-external@goironfort.com` is a managed Google Group containing only authorized IronFort compliance specialists. IronFort controls membership in this group and keeps it up to date.

Do I need to repeat this for multiple projects? Yes. Repeat these steps for each Google Cloud project you want IronFort to review.

Need Help?

If you have any questions or need assistance with these steps, please reach out to us.

Email: hello@goironfort.com

We're happy to walk you through the setup or answer any questions you may have.