Google Cloud

Assured Workloads Quick Start Guide

Assured Workloads Overview

Assured Workloads allows Google Cloud customers to easily configure and maintain controlled environments that operate within the parameters of a specific compliance regime. Assured Workloads is a modern government cloud solution that allows public sector customers to run regulated workloads on Google Cloud's public cloud infrastructure. Assured Workloads uses a set of platform controls to create regulated boundaries on Google Cloud and support compliance workloads including, but not limited to: FedRAMP Moderate, FedRAMP High, IL4/5, IRS 1075, CJIS, and ITAR. Please review our platform controls page for the full list of supported compliance frameworks.

Purpose

This guide walks through the key steps on how to set up and evaluate the core capabilities of Assured Workloads in your Google Cloud environment. For a complete set of product how-to-guides and API reference, please visit the Assured Workloads documentation.

Google Cloud

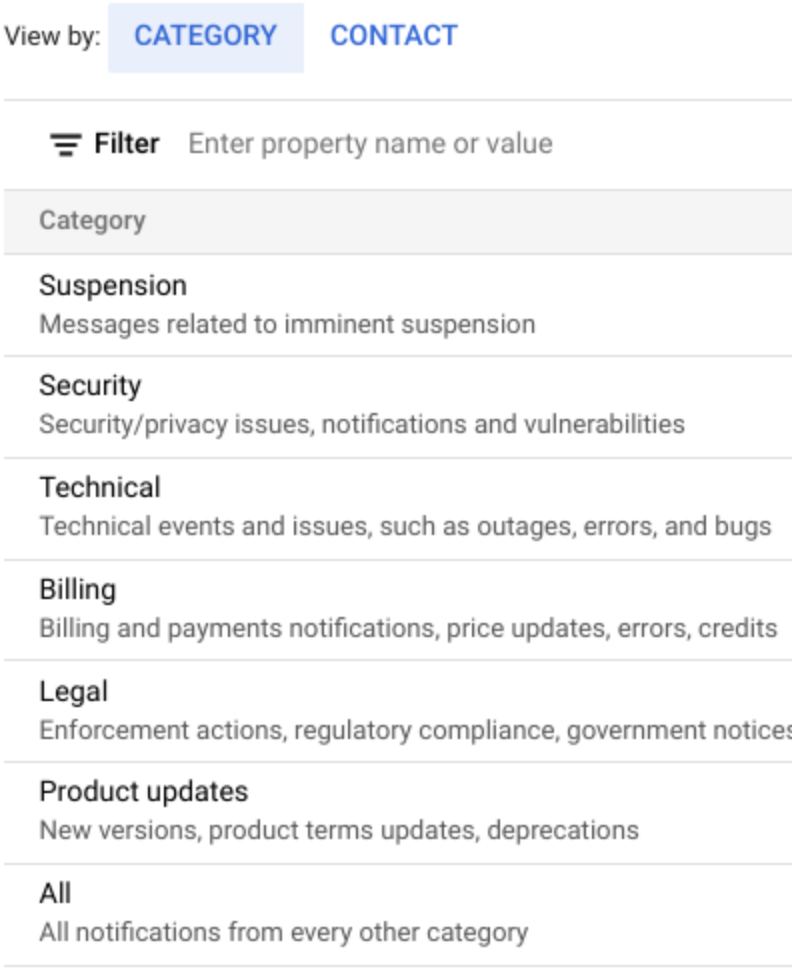
Step 0: Set Up Essential Contacts

Many Google Cloud services send out notifications to share important information with Google Cloud users. With Essential Contacts, you can customize who receives notifications by providing your own list of contacts. This is important because different individuals and teams within your organization care about different types of notifications. To reduce the impact of personnel changes, we recommend adding groups as contacts, then managing the membership of those groups to determine who receives notifications. This practice helps ensure that notifications always go to active employees.

- To set up Essential Contacts, you need the following Identity and Access Management (IAM) roles:
  - Essential Contacts Admin: roles/essentialcontacts.admin
- Enable the Essential Contacts API
- Visit the Essential Contacts page
- Ensure the Google Cloud Organization is selected
- Add an Essential Contact for **Legal**

We recommend adding three Contacts for the Legal category: representatives from your Legal, Compliance, and Security departments. **This group will receive notifications of compliance violations**, so this will ensure that Legal and Compliance remain informed, and acts as an immediate notification to Security for remediation actions.

Please visit this page for more information and best practices on Essential Contacts.

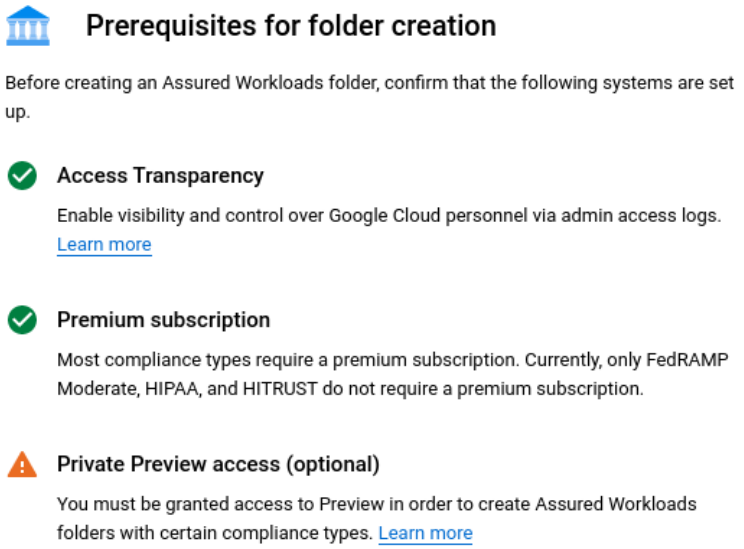


Google Cloud

Step 1: Set Up the Assured Workloads Prerequisites

- To set up Assured Workloads, you need the following IAM roles:
  - Access Transparency Admin: roles/axt.admin
  - Assured Workloads Admin: roles/assuredworkloads.admin
  - Resource Manager Organization Viewer: roles/resourcemanager.organizationViewer
- If you will use Premium Platform Controls:
  - Ensure you have Enhanced or Premium Support
  - Enable Access Transparency
- If you wish to use Assured Workloads Premium Platform Controls but don't currently have a Premium subscription:
  - Sign-up for a 60-day Premium Free Trial

Watch this video to view a set up of Assured Workloads.

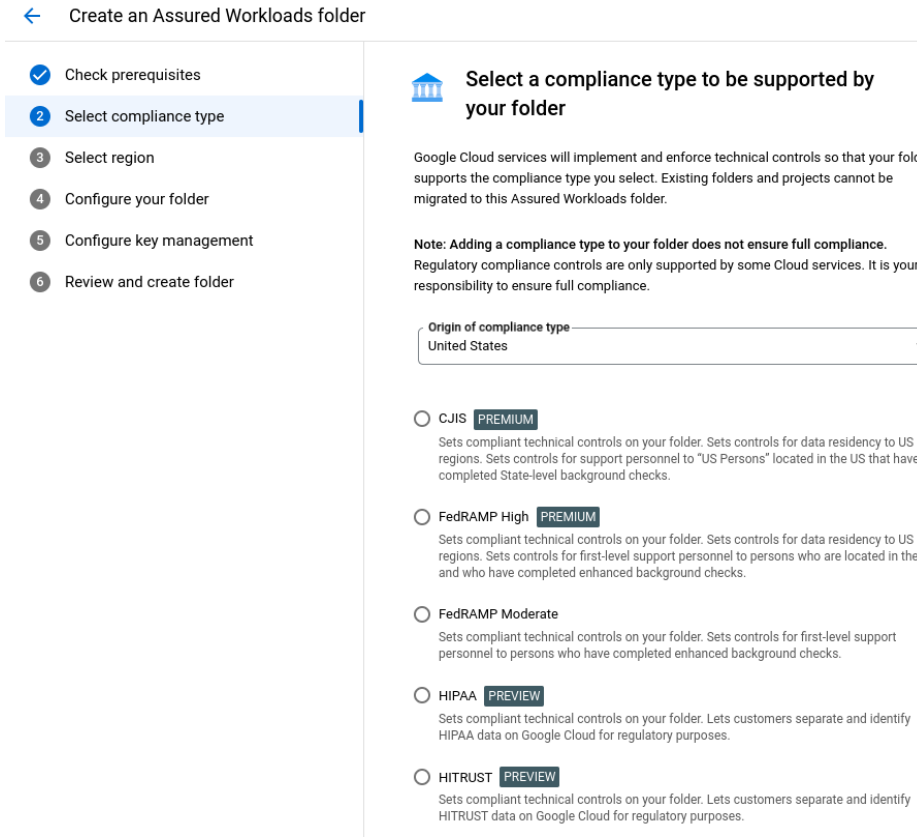


Google Cloud

Step 2: Create an Assured Workloads Folder

Assured Workloads implements and enforces technical controls within your folders to help you comply with a particular compliance framework or set of requirements. Any folder or project created inside of one of your Assured Workloads folders will inherit the guardrails you specified.

- Visit the Assured Workloads Console
- Create an Assured Workloads Folder based on the desired Compliance type and desired jurisdiction
- Configure your Key Management Project and Key Ring. This creates a storage location for your cryptographic keys, not the keys themselves.
    - Configuring a Key Management Project and Key Ring is **only** required for CJIS and ITAR workloads.
    - Creating an EU Regions and Support with Sovereignty Controls requires enabling Key Access Justifications **before** folder creation, and subsequently enabling Signed Access Approval **after** folder creation.
- Return to the Assured Workloads console.
- Click on the folder name and verify the folder was created with the details you specified.



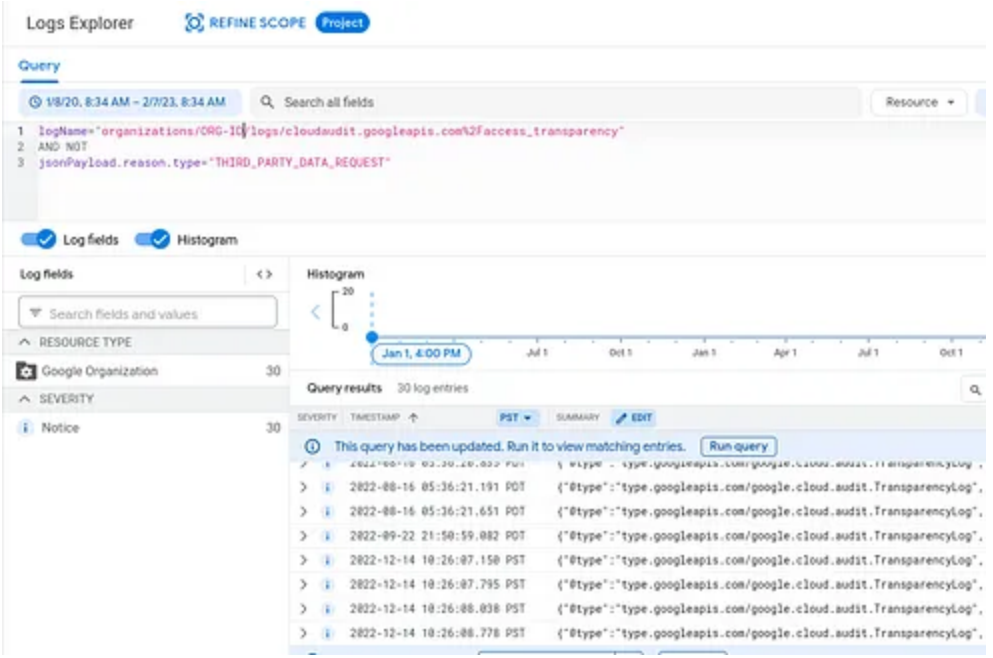
Google Cloud

Step 3: Monitor Access Transparency Logs

Access Transparency aims to provide customers progressively greater transparency and control over access to their content stored in Google Cloud.

- Set controls for who can access the Access Transparency logs by assigning a user or group the **Private Logs Viewer** role: roles/logging.privateLogViewer
- Visit Cloud Logging. Use the Logs Explorer to filter for logs. Example queries are highlighted here.
- Create a logs-based metric and then set up an alerting policy to give you timely awareness of issues surfaced by these logs.

Watch this video on using Cloud Logging to understand how actions are logged.



Google Cloud

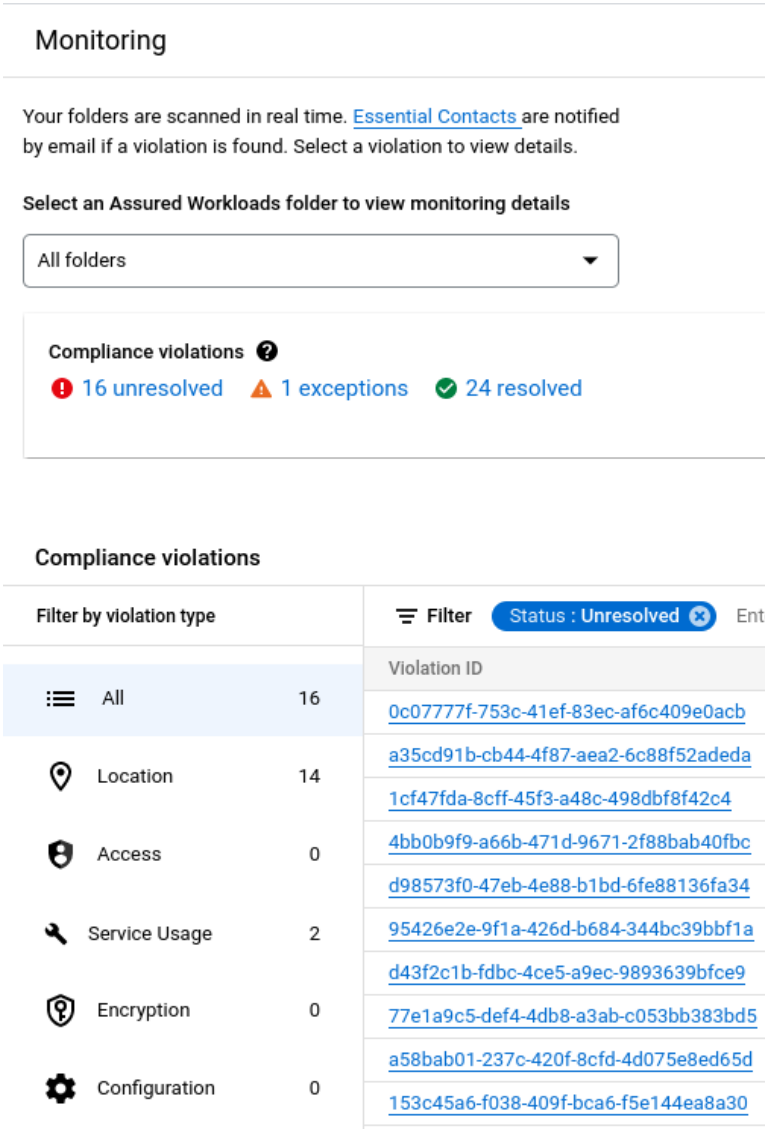
Step 4: Discover Compliance Violations

Assured Workloads monitors a compliance regime's organization policy constraints, and highlights a violation if a change to a resource is non-compliant. You can then resolve these violations, or create exceptions for them where appropriate.

Monitor the organization policy constraints, and highlight violations if a change to a resource is non-compliant.

- Return to the Assured Workloads Console
- Navigate to Monitoring to view the status of your compliance violations
- To view these violations, click the **Violation ID** tab.
- Take action and remediate these violations by following the remediation steps in the **Violation Details**

Please visit this page for the complete list of Monitored Violations.



Google Cloud

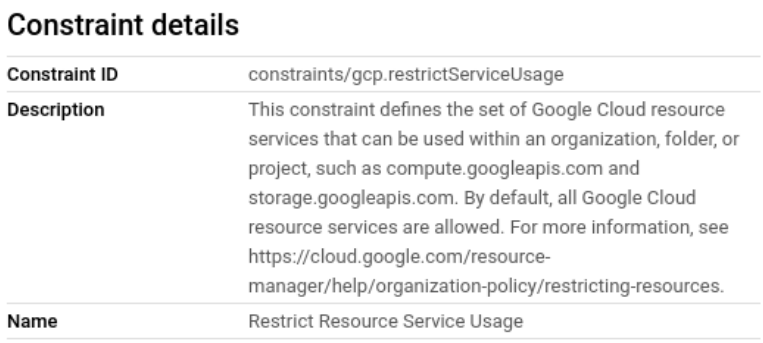
Optional Steps

These steps should only be used as necessary, and are not required for most Assured Workloads customers.

Step 5: Exceptions to Resource Usage Restrictions Policy

You can selectively disable restrictions that prevent the usage of resources that aren't compliant with certain compliance regimes. **This is not recommended because it makes the Assured Workloads folder less restrictive and puts your environment in non-compliant scope**. However, it is available to customers who accept the risk of using non-compliant products.

- Ensure you have the appropriate IAM roles:
  - Org Policy Administrator: roles/orgpolicy.policyAdmin
  - Assured Workloads Admin: roles/assuredworkloads.admin
- Modify the policy based on these instructions
- Add an Assured Workloads Monitoring Violation Exception to ensure the change has a documented business justification and isn't reported as "Unresolved"



Constraint details

Constraint ID	constraints/gcp.restrictServiceUsage
Description	This constraint defines the set of Google Cloud resource services that can be used within an organization, folder, or project, such as compute.googleapis.com and storage.googleapis.com. By default, all Google Cloud resource services are allowed. For more information, see https://cloud.google.com/resource-manager/help/organization-policy/restricting-resources.
Name	Restrict Resource Service Usage

We recommend maintaining Organization Policy Restrictions in place, as they help restrict access to unauthorized services and regions. For an introduction on Organization Policy Restrictions, please watch this video. For more information on Restriction Resource Usage for Assured Workloads, including limitations, please read this guide.

Step 6: Restrict TLS Versions

Google Cloud supports multiple TLS protocol versions. To meet compliance requirements, you may want to deny handshake requests from clients that use older TLS versions.

- Ensure you have the appropriate IAM role:
  - Org Policy Administrator: roles/orgpolicy.policyAdmin
- Follow this guide to restrict certain TLS versions

Google Cloud

Step 7: Register Representative for the GDPR

If your organization is required to appoint a data protection officer (DPO), an EU representative, or both, in accordance with the European Union's (EU) General Data Protection Regulation (GDPR), register their details in your Google Admin console.

- Follow this guide to register your representatives.