Google Cloud

Assured Workloads: Australia Regions and Assured Support Quick Start Guide

Assured Workloads Overview

Assured Workloads is a modern government cloud solution that allows customers to run regulated workloads on Google Cloud's public cloud infrastructure. Assured Workloads allows Google Cloud customers to easily configure and maintain controlled environments that operate within the parameters of a specific compliance program. Assured Workloads' Australia Regions with Assured Support program meets the requirements of the Australian government's Information Security Registered Assessors Program (IRAP) and the Hosting Certification Framework (HCF), which is administered by the Digital Transformation Agency.

Google Cloud

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.

View by: **CATEGORY**   **CONTACT**

≡ Filter   Enter property name or value

Category

Suspension
Messages related to imminent suspension

Security
Security/privacy issues, notifications and vulnerabilities

Technical
Technical events and issues, such as outages, errors, and bugs

Billing
Billing and payments notifications, price updates, errors, credits

Legal
Enforcement actions, regulatory compliance, government notices

Product updates
New versions, product terms updates, deprecations

All
All notifications from every other category

For more information visit **cloud.google.com/assured-workloads**

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 Compliance Programs:
  - Ensure you have Enhanced or Premium Support
  - Enable Access Transparency
- If you wish to use Assured Workloads Premium Compliance Programs but don't currently have a Premium subscription:
  - Sign-up for a 60-day Premium Free Trial

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

Prerequisites for folder creation

Before creating an Assured Workloads folder, confirm that the following systems are set up.

✅ **Access Transparency**

Enable visibility and control over Google Cloud personnel via admin access logs. Learn more ↗

⚠️ **Private Preview access (optional)**

You must be granted access to Preview in order to create Assured Workloads folders with certain compliance types. Learn more ↗

ⓘ **Enhanced or Premium Support**

Enhanced or Premium Support is required to use Assured Support for all compliance types. Purchase support ↗

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:
    a. In the "Origin of Compliance Type" select "Australia"
    b. Click on "Australia Regions with Assured Support"
- Select a region based on the desired location
- Select your folder location and name your folder
- Configure your Key Management Project and Key Ring. This creates a storage location for your cryptographic keys, not the keys themselves.
- Review the details of your folder and click "Create"

🏛 **Select a compliance type to be supported by your folder**

Google Cloud services will implement and enforce technical controls so that your folder supports the compliance type you select. Existing folders and projects cannot be migrated to this Assured Workloads folder.

Note: Adding a compliance type to your folder does not ensure full compliance. Regulatory compliance controls are only supported by some Cloud services. It is your responsibility to ensure full compliance.

Origin of compliance type
Australia   ▾

◉ Australia Regions with Assured Support

Assured Support provides customers 24/7 access to Google Cloud technical support from 5 specific countries (United States, Canada, Australia, United Kingdom, and New Zealand). Support is provided in English language. Sets data location controls to available Australia regions.

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
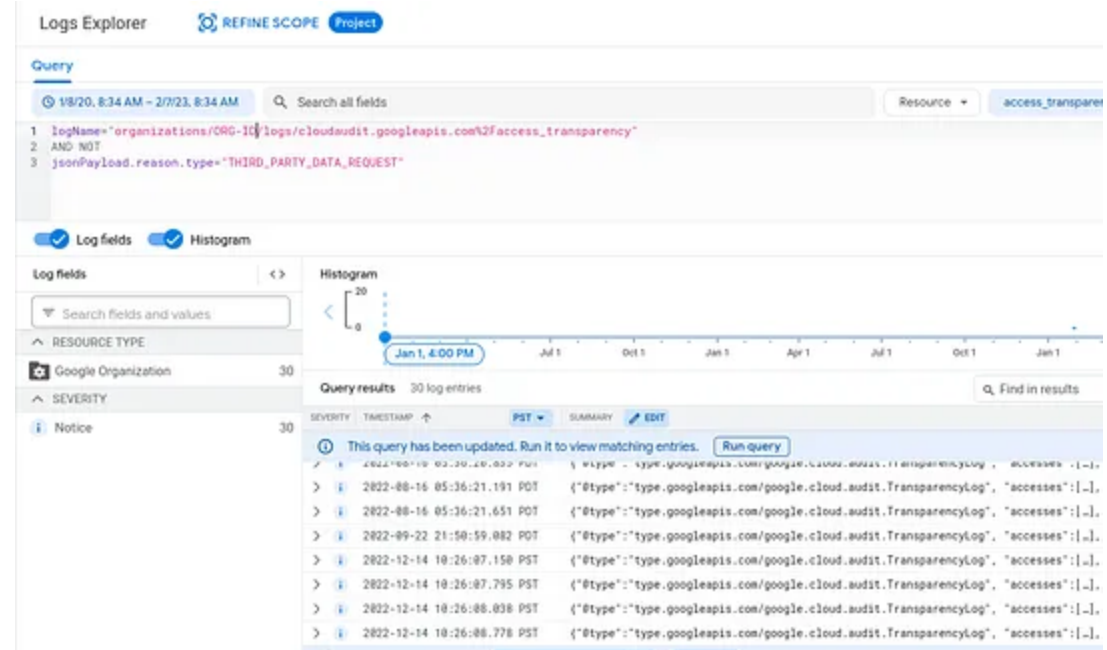
Step 4: Discover Compliance Violations

Assured Workloads monitors a compliance program'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.

Monitoring

Your folders are scanned in real time. [Essential Contacts](#) are notified by email if a violation is found. Select a violation to view details.

Select an Assured Workloads folder to view monitoring details

All folders ▼

Compliance violations ❓

🛑 16 unresolved   ⚠️ 1 exceptions   ✅ 24 resolved

Compliance violations

Filter by violation type		☰ Filter Status : Unresolved ⊗ Ent
☰ All	16	**Violation ID**
		0c07777f-753c-41ef-83ec-af6c409e0acb
📍 Location	14	a35cd91b-cb44-4f87-aea2-6c88f52adeda
		1cf47fda-8cff-45f3-a48c-498dbf8f42c4
🛡️ Access	0	4bb0b9f9-a66b-471d-9671-2f88bab40fbc
		d98573f0-47eb-4e88-b1bd-6fe88136fa34
🔧 Service Usage	2	95426e2e-9f1a-426d-b684-344bc39bbf1a
		d43f2c1b-fdbc-4ce5-a9ec-9893639bfce9
🔏 Encryption	0	77e1a9c5-def4-4db8-a3ab-c053bb383bd5
		a58bab01-237c-420f-8cfd-4d075e8ed65d
⚙️ Configuration	0	153c45a6-f038-409f-bca6-f5e144ea8a30

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 the Resource Location Policy

You can selectively add additional Australian regions to ensure that your applications are more resilient.
- 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"

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.

Constraint details

Constraint ID	constraints/gcp.resourceLocations
Description	This list constraint defines the set of locations where location-based Google Cloud resources can be created. By default, resources can be created in any location. Policies for this constraint can specify multi-regions such as `asia` and `europe`, regions such as `us-east1` or `europe-west1` as allowed or denied locations. Allowing or denying a multi-region does not imply that all included sub-locations should also be allowed or denied. For example, if the policy denies the us multi-region (which refers to multi-region resources, like some storage services), resources can still be created in the regional location `us-east1`. On the other hand, the `in:us-locations` group contains all locations within the us region, and can be used to block every region. We recommend using value groups to define your policy.

Google Cloud

Step 6: Exceptions to Restrict Service Usage Policy

You can selectively disable restrictions that prevent the usage of resources that aren't compliant with certain compliance programs. **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 the desired Australian region
- Add an Assured Workloads Monitoring Violation Exception to ensure the change has a documented business justification and isn't reported as "Unresolved"

For more information on Restriction Resource Usage for Assured Workloads, including limitations, please read this guide.

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

Step 7: 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

Constraint details

Constraint ID	constraints/gcp.restrictTLSVersion
Description	This constraint defines the set of TLS versions that cannot be used on the organization, folder, or project where this constraint is enforced, or any of that resource's children in the resource hierarchy. By default, all TLS versions are allowed. TLS versions can only be specified in the denied list, and must be identified in the form TLS_VERSION_1 or TLS_VERSION_1_1.This constraint is only applied to requests using TLS. It will not be used to restrict unencrpyted requests. For more information, see https://cloud.google.com/assured-workloads/docs/restrict-tls-versions.

For more information visit **cloud.google.com/assured-workloads**