

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](#).

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

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/resourcecmanager.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](#).



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](#)



Premium subscription

Most compliance types require a premium subscription. Currently, only FedRAMP Moderate, HIPAA, and HITRUST do not require a premium subscription.



Private Preview access (optional)

You must be granted access to Preview in order to create Assured Workloads folders with certain compliance types. [Learn more](#)

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.

← Create an Assured Workloads folder

- ✓ Check prerequisites
- 2 Select compliance type
- 3 Select region
- 4 Configure your folder
- 5 Configure key management
- 6 Review and create folder

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
United States

- CJIS **PREMIUM**
Sets compliant technical controls on your folder. Sets controls for data residency to US regions. Sets controls for support personnel to "US Persons" located in the US that have completed State-level background checks.
- FedRAMP High **PREMIUM**
Sets compliant technical controls on your folder. Sets controls for data residency to US regions. Sets controls for first-level support personnel to persons who are located in the and who have completed enhanced background checks.
- FedRAMP Moderate
Sets compliant technical controls on your folder. Sets controls for first-level support personnel to persons who have completed enhanced background checks.
- HIPAA **PREVIEW**
Sets compliant technical controls on your folder. Lets customers separate and identify HIPAA data on Google Cloud for regulatory purposes.
- HITRUST **PREVIEW**
Sets compliant technical controls on your folder. Lets customers separate and identify HITRUST data on Google Cloud for regulatory purposes.

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.

The screenshot displays the Google Cloud Logs Explorer interface. At the top, it shows 'Logs Explorer' with a 'REFINE SCOPE' button and a 'Project' dropdown. Below this is a 'Query' section with a search bar and a 'Resource' dropdown. The query text is:

```
1 logName="organizations/ORG-ID/logs/cloudaudit.googleapis.com%2Faccess_transparency"
2 AND NOT
3 jsonPayload.reason.type="THIRD_PARTY_DATA_REQUEST"
```

Below the query, there are two tabs: 'Log fields' and 'Histogram'. The 'Log fields' tab is active, showing a search bar and a list of fields: 'RESOURCE TYPE' (Google Organization, 30), and 'SEVERITY' (Notice, 30). The 'Histogram' tab shows a timeline view with a peak at 'Jan 1, 4:00 PM'. Below the histogram, it says 'Query results: 30 log entries'. A table of results is shown with columns for 'SEVERITY', 'TIMESTAMP', 'PST', 'SUMMARY', and 'EDIT'. The first row is highlighted, showing a timestamp of '2022-08-16 05:36:21.191 PDT' and a summary of 'type.googleapis.com/google.cloud.audit.TransparencyLog'. A notification banner at the bottom of the results table says 'This query has been updated. Run it to view matching entries.' with a 'Run query' button.

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.

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

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"

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](#)

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: 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.