# 

**CSWG- Policy As Code Documentation**

Cloud Storage Sentinel Policies

5.1 Ensure That Cloud Storage Bucket Is Not Anonymously or Publicly Accessible (Automated)

***Sentinel Policy Name:***

* + 5.1 Ensure That Cloud Storage Bucket Is Not Anonymously or Publicly Accessible (Automated).

***Category:***

* + Cloud Storage

***Description of Policy:***

* + Allowing anonymous or public access grants permissions to anyone to access bucket content.
  + Such access might not be desired if you are storing any sensitive data. Hence, ensure that anonymous or public access to a bucket is not allowed.

***Terraform Providers:***

<https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/storage_bucket_iam>  - resource block “google\_storage\_bucket\_iam\_binding” or “google\_storage\_bucket\_iam\_policy” or “google\_storage\_bucket\_iam\_member” can be used.

***Sentinel Policy Restriction:***

* + In this sentinel policy, “members” parameter should not be set to “allUsers” and “allAuthenticatedUsers”.

***Pass and fail cases of above sentinel policy:***

**Pass Case:**

1. “members” parameter should not be set to “allUsers” and “allAuthenticatedUsers”.

"members " : 
" user : user@example.com", 

**Fail Case:**

1. “members” parameter should be set to “allUsers” and “allAuthenticatedUsers”.

"members " : 
" allAuthenticatedUsers " , 
"allUsers " , 

**Testcases Output:**

PS C: \Users\1939847\Documents\c10ud storage\Ensure-anonymous> sentinel test 
PASS - ensure-storage-bucket-is-not-anonymously-accessible. sentinel 
PASS - test\ensure-storage-bucket-is-not-anonymously-accessible\fail.hcl 
PASS - test\ensure-storage-bucket-is-not-anonymously-accessible\pass.hcl 

5.2 Ensure That Cloud Storage Buckets Have Uniform Bucket-Level Access Enabled (Automated).

***Sentinel Policy Name:***

* + 5.2 Ensure That Cloud Storage Buckets Have Uniform Bucket-Level Access Enabled (Automated).

***Category:***

* + Cloud Storage

***Description of Policy:***

* + It is recommended to use uniform bucket-level access to unify and simplify how you grant access to your Cloud Storage resources.
  + Cloud Storage offers two systems for granting users permission to access your buckets and objects: Cloud Identity and Access Management (Cloud IAM) and Access Control Lists (ACLs).
  + Cloud IAM is used throughout Google Cloud and allows you to grant a variety of permissions at the bucket and project levels. ACLs are used only by Cloud Storage and have limited permission options, but they allow you to grant permissions on a per-object basis.
  + In order to support a uniform permissioning system, Cloud Storage has uniform bucket level access.

***Terraform Providers:***

<https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/storage_bucket> - resource block “google\_storage\_bucket” is used.

***Sentinel Policy Restriction:***

* + In this sentinel policy, “uniform\_bucket\_level\_access” parameter is set to “true”.

***Pass and fail cases of above sentinel policy:***

**Pass Case:**

1. uniform\_bucket\_level\_access” parameter is set to “true”.

"uniform bucket level access": 
true, 

**Fail Case:**

1. uniform\_bucket\_level\_access” parameter is set to “false”.

"uniform bucket level access" : 
false, 

**Testcases Output:**

PS C: storage\Ensure-uniform-bucket-1eve1-is-enab1ed> sentinel test 
PASS - Ensure-uniform-bucket-level-is-enabled. sentinel 
PASS - test\Ensure-uniform-bucket-1eve1-is-enab1ed\fai1.hc1 
PASS - test\Ensure-uniform-bucket-1eve1-is-enab1ed\pass.hc1 