ant: Uniform bucket-level access was known as Bucket Policy Only during Beta. The organization policy and API fiel
ng to Bucket Policy Only are still supported, but we recommend using the equivalent uniform bucket-level access
zation policy and API fields.

This page shows you how to enable, disable and check the status of uniform bucket-level access on a bucket in Cloud Storage. For details about this feature, see Uniform bucket-level access (/storage/docs/uniform-bucket-level-access).

Before using this feature in Cloud Storage, you should:

1. Have sufficient permission to view and update buckets in Cloud Storage:
    - If you own the project that contains the bucket, you most likely have the necessary permissions.
    - You should have the `storage.buckets.update` and `storage.buckets.get` IAM permissions on the relevant bucket. See Using IAM Permissions (/storage/docs/access-control/using-iam-permissions) for instructions on how to get a role, such as `roles/storage.admin`, that has these permissions.

Before you enable uniform bucket-level access, use Stackdriver to ensure your bucket is not using ACLs for any workflows. For more information, see Check object ACL usage (/storage/docs/uniform-bucket-level-access#acl-check).

ant: Once uniform bucket-level access has been enabled on a bucket for 90 consecutive days, it can no longer be dis

To enable uniform bucket-level access on your bucket:

ant: Once uniform bucket-level access has been enabled on a bucket for 90 consecutive days, it can no longer be dis

You must remove all Cloud IAM conditions (/storage/docs/access-control/using-iam-permissions#conditions-remove) from the bucket's Cloud IAM policy before you can disable uniform bucket-level access.

To disable uniform bucket-level access on your bucket:

- Learn more about uniform bucket-level access (/storage/docs/uniform-bucket-level-access).
- Set IAM permissions on buckets and projects (/storage/docs/access-control/using-iam-permissions).