You can control who has access to your Cloud Storage buckets and objects as well as what level of access they have. Below is a summary of the access control options available to you, along with links to learning more about each:

- Cloud Identity and Access Management (Cloud IAM) permissions (/storage/docs/access-control/iam): Grant access to buckets as well as bulk access to a bucket's objects. Cloud IAM permissions give you broad control over your projects and buckets, but not fine-grained control over individual objects. For a reference of Cloud IAM permissions and roles specific to Cloud Storage, as well as which permissions allow users to run JSON and XML methods on buckets and objects, see the Cloud IAM Reference pages (/storage/docs/access-control/iam-reference). To learn how to use Cloud IAM permissions, see Using Cloud IAM Permissions (/storage/docs/access-control/using-iam-permissions).

- Access Control Lists (ACLs) (/storage/docs/access-control/lists): Grant read or write access to users for individual buckets or objects. In most cases, you should use Cloud IAM permissions instead of ACLs. Use ACLs only when you need fine-grained control over individual objects. To learn how to use ACLs, see Create and Manage Access Control Lists (/storage/docs/access-control/create-manage-lists).

- Signed URLs (query string authentication) (/storage/docs/access-control/signed-urls): Give time-limited read or write access to an object through a URL you generate. Anyone with whom you share the URL can access the object for the duration of time you specify, regardless of whether or not they have a Google account. Learn how to create signed URLs:

  - with gsutil or client libraries (/storage/docs/access-control/signing-urls-with-helpers).

  - with a program (/storage/docs/access-control/signing-urls-manually).

- Signed Policy Documents (/storage/docs/xml-api/post-object#policydocument): Specify what can be uploaded to a bucket. Policy documents allow greater control over size, content type, and other upload characteristics than signed URLs, and can be used by website owners to allow visitors to upload files to Cloud Storage.

- Firebase Security Rules (https://firebase.google.com/docs/storage/security): Provide granular, attribute-based access control to mobile and web apps using the Firebase SDKs for Cloud Storage (https://firebase.google.com/docs/storage). For example, you can specify who can upload or download objects, how large an object can be, or when an object can be downloaded.

These options are not mutually exclusive. For example, you can use ACLs to generally give private access to a bucket, but then create a signed URL or policy document that allows anyone you choose to access a resource within the bucket, bypassing the ACL mechanism.

For examples of sharing and collaboration scenarios that involve setting bucket and object ACLs, see Sharing and Collaboration (/storage/docs/collaboration).