This page describes how to control access to buckets and objects using Cloud Identity and Access Management (Cloud IAM) permissions. Cloud IAM allows you to control who has access to your buckets and objects. To learn more about Cloud IAM for Cloud Storage, see the Overview of Cloud IAM (/storage/docs/access-control/iam).

To learn about other ways to control access to buckets and objects, read Overview of Access Control (/storage/docs/access-control/index). To learn about controlling access to individual objects in your buckets, see Access Control Lists (/storage/docs/access-control/lists).

Cloud IAM policies cannot be managed using the XML API. Cloud IAM policies containing Cloud IAM Conditions age/docs/access-control/iam#conditions)BETA cannot be managed using client libraries.

The following sections show how to complete basic Cloud IAM tasks on buckets.

For a list of roles associated with Cloud Storage, see Cloud IAM Roles (/storage/docs/access-control/iam-roles). For information on entities to which you grant Cloud IAM roles, see Member Types (/storage/docs/access-control/iam#identities).

You should set the minimum permission possible that gives the member the required access. For example, if the tean
er only needs to read objects stored in a bucket, select the **Storage Object Viewer** role. Similarly, if the team member
ntrol of objects in the bucket (but not control of the bucket itself), select **Storage Object Admin**.

Some roles may not appear in the bucket permissions window. If you assign roles at the project level, they do not app
cket permission window, even when users with that role have access to your bucket. To view these project-level
ssions, go to the **IAM & Admin** screen (https://console.cloud.google.com/iam-admin/projects).

tant: It typically takes about a minute for revoking access to take effect. In some cases it may take longer. If you rem access, this change is immediately reflected in the metadata; however, the user may still have access to the object fo period of time.

eature is in a pre-release state and might change or have limited support. For more information, see the product launc s (/products/#product-launch-stages).

The following sections show you how to add and remove Cloud IAM Conditions (/iam/docs/conditions-overview) on your buckets. To view the Cloud IAM Conditions for your bucket, see Viewing the Cloud IAM policy for a bucket (/storage/docs/access-control/using-iam-permissions#bucket-view). For more information about using Cloud IAM Conditions with Cloud Storage, see Conditions (/storage/docs/access-control/iam#conditions).

You must enable uniform bucket-level access (/storage/docs/using-uniform-bucket-level-access#enable) on the bucket before adding conditions.

The following sections show how to complete basic Cloud IAM tasks on projects. Note that these tasks use a separate command line command, `gcloud`, and a separate endpoint, `cloudresourcemanager.googleapis.com`, compared to most Cloud Storage tasks.

To complete the following tasks, you must have the `resourcemanager.projects.getIamPolicy` and `resourcemanager.projects.setIamPolicy` Cloud IAM permissions.

For a list of roles associated with Cloud Storage, see Cloud IAM Roles (/storage/docs/access-control/iam-roles). For information on entities to which you grant Cloud IAM roles, see Member Types (/storage/docs/access-control/iam#identities).

You should set the minimum permission possible that gives the member the required access. For example, if the team
er only needs to read objects stored in a project, select the **Storage Object Viewer** permission. Similarly, if the team
er needs full control of objects (but not buckets) in a project, select **Storage Object Admin**.

tant: It typically takes about a minute for revoking access to take effect. In some cases it may take longer. If you rem access, this change is immediately reflected in the metadata; however, the user may still have access to the object fo period of time.

- Learn how to publicly share your data (/storage/docs/access-control/making-data-public).
- Learn more about Cloud IAM in Cloud Storage (/storage/docs/access-control/iam).
- See specific Sharing and collaboration examples (/storage/docs/collaboration).
- Learn about options to control access to your data (/storage/docs/access-control/index).