

Controlling access to tables and views

ature is covered by the [Pre-GA Offerings Terms \(/terms/service-terms#1\)](/terms/service-terms#1) of the Google Cloud Platform Terms a. Pre-GA features may have limited support, and changes to pre-GA features may not be compatible with other versions. For more information, see the [launch stage descriptions \(/products#product-launch-stages\)](/products#product-launch-stages).

This page shows you how to use BigQuery Table ACL to control access to tables and views. For an overview of BigQuery Table ACL, see [Introduction to table access controls \(/bigquery/docs/table-access-controls-intro\)](/bigquery/docs/table-access-controls-intro).

After you create a table or view, you can set its policy in the following ways:

- using the BigQuery web UI
- using the `bq set-iam-policy` command
- calling the `tables.setIamPolicy` method

You can use BigQuery Table ACL to set access on both logical views and dataset-level authorized views. A logical view can also reference other source tables and views that you shared using BigQuery Table ACL.

Before you begin

1. Create the [table \(/bigquery/docs/tables#create-table\)](/bigquery/docs/tables#create-table) or [view \(/bigquery/docs/views#creating_a_view\)](/bigquery/docs/views#creating_a_view) that you want to use with BigQuery Table ACL.
2. Grant the BigQuery Data Owner (`roles/bigquery.dataOwner`) role or the BigQuery Admin (`roles/bigquery.admin`) role to the person that will perform the steps in this topic.

Creating an access policy

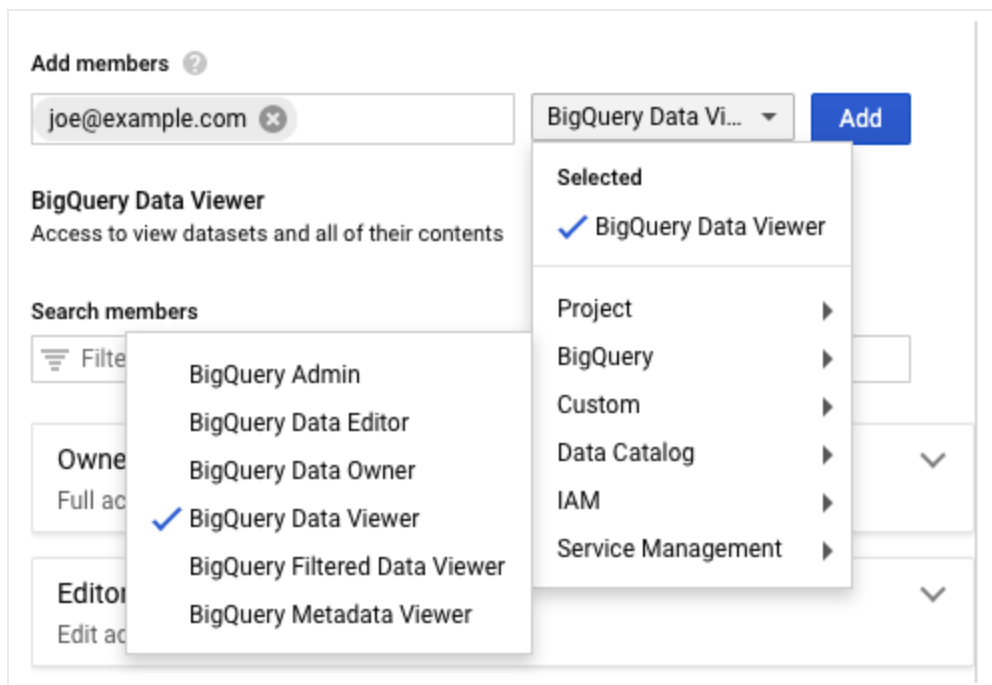
To create an access policy on a table or view:

Console [#bq](#) API [#api](#)

1. Open the BigQuery web UI in the Cloud Console.

[Go to the Cloud Console](https://console.cloud.google.com/bigquery) (<https://console.cloud.google.com/bigquery>)

2. In the navigation panel, in the **Resources** section, select your project.
3. Select the dataset that contains the table or view.
4. Select the table or view.
5. If you are modifying access for a table, click **Share table**. If you are modifying access for a view, click **Share view**.
6. The **Table permissions** or **View permissions** page opens. For **Add members**, enter the email address of the user that will receive access to the table or view.
7. From the **Select a role** dropdown, select the role that you want to grant to the user. The following shows granting `joe@example.com` to the BigQuery Data Viewer (`roles/bigquery.dataViewer`) role.



8. Click **Done**.

After you create a policy, subsequent retrieval of the policy will show that its version field is 1. Do not change the version number. This version number refers to the IAM policy schema version, not your version of the table policy. For information about IAM policy schema versions, see [Policy versions](https://iam/docs/policies#versions) ([/iam/docs/policies#versions](https://iam/docs/policies#versions)).

For more information about Identity and Access Management policies, see [Understanding policies \(/iam/docs/policies\)](/iam/docs/policies) and the [Policy \(/iam/docs/reference/rest/v1/Policy\)](/iam/docs/reference/rest/v1/Policy) reference topic.


Updating an access policy

To update an access policy on a table or view:

[Console](#)[bq. \(#bq\)](#)[API \(#api\)](#)

1. Open the BigQuery web UI in the Cloud Console.

[Go to the Cloud Console \(https://console.cloud.google.com/bigquery\)](https://console.cloud.google.com/bigquery)

2. In the navigation panel, in the **Resources** section, select your project.
3. Select the dataset that contains the table or view.
4. Select the table or view.
5. If you are modifying access for a table, click **Share table**. If you are modifying access for view, click **Share view**.
6. The **Table permissions** or **View permissions** page opens.
 - If you want to add new members, use the same technique shown in [Creating an access policy \(#create\)](#).
 - If you want to remove access for a user, search for the user by using the **Search members** field. For each group where you want to remove the user, expand the group, and then click the **Delete**  button for the user.
 - If you want to change group membership for a user, make additions and/or deletions as described in the immediate 2 steps above.
7. Repeat as needed for other users whose access you want to add, modify, or remove. When you are done, click **Done**.

For more information about Identity and Access Management policies, see [Understanding policies \(/iam/docs/policies\)](/iam/docs/policies) and the [Policy \(/iam/docs/reference/rest/v1/Policy\)](/iam/docs/reference/rest/v1/Policy) reference topic.

What's next

- Read the [FAQ \(/bigquery/docs/table-access-controls-faq\)](/bigquery/docs/table-access-controls-faq).
- Learn about audit logging of BigQuery Table ACL admin activities at [Audit logging \(/bigquery/docs/table-access-controls-intro#audit_logging\)](/bigquery/docs/table-access-controls-intro#audit_logging).

Except as otherwise noted, the content of this page is licensed under the [Creative Commons Attribution 4.0 License \(https://creativecommons.org/licenses/by/4.0/\)](https://creativecommons.org/licenses/by/4.0/), and code samples are licensed under the [Apache 2.0 License \(https://www.apache.org/licenses/LICENSE-2.0\)](https://www.apache.org/licenses/LICENSE-2.0). For details, see the [Google Developers Site Policies \(https://developers.google.com/site-policies\)](https://developers.google.com/site-policies). Java is a registered trademark of Oracle and/or its affiliates.

Last updated 2020-07-21 UTC.