API permissions

Flow provides object-level permissions.

In general, you should create an API service account rather than mapping the API to an individual. Typically, you name that service account something generic like `API_SERVICE_ACCOUNT`.

Permissions

You need Manage API keys permissions to manage API keys.

Read more about Flow roles and permissions.

View rights and API

View Rights are a key feature in Flow to control the depth of information a user can see in Flow's interface. To learn more about View Rights, visit types of view rights.

However, view rights are completely bypassed in the API. This is by design.

View Rights are report dependent. The API is based on primitive objects, not reports. This is important to understand as it has serious security and information access implications.

If you give a person access to the COMMITS object in the API, for example, they will have complete unrestricted access to that object. This means they will be able to see any commit in any team in any repo.

If you wish to restrict or control that access, you must enforce it at the client level. This is in part why we strongly recommend you use a service account.
Assigning API permissions

To assign API permissions:

1. In the top navigation bar and click Settings.

2. In the left navigation under User Management, click Users.

3. Locate and select the user you wish to give API permissions to.

4. On the User detail page, click the Access tab.

5. In the Access tab, select any API-related roles and permissions you want to assign to the user:
   
   - In the Management section, make sure Manage API keys is checked to allow the user to create, assign, and deactivate API keys.
   - In the API access tab, select the APIs objects from which users can request data. If the user accesses the Flow API from a REST client or uses an application to integrate Flow data, they need an API key. See Authentication.

6. Click Save Changes.

If you need help, please email support@pluralsight.com for 24/7 assistance.