API Key Overview

- API keys are used to authenticate requests to the Resolver Core API without entering user credentials.
- API keys never expire, with no need to establish or maintain a session.
- API keys are tied to the user's org account. This means that if a user doesn't have permission to perform an action in Core, they won't be able to do it through the API.
- Only admins and super admins can create API keys. Admins can only create keys for orgs on which they're an admin.
- For security purposes, API keys are not stored. If you misplace the key, it cannot be retrieved and must be regenerated.
- It's possible to create API keys to impersonate other users; however, only super admins can enable this feature. See the **Impersonation** section of Use an API Key article for more information.
- Only active users of the same org as the API key user can be impersonated.
- Any call can be made using an API key while impersonating another user; however, only three endpoints in the Swagger user interface support this:

    - **POST** /data/file/file in the **file** resource;
    - **POST** /data/object/{objectID}/file/{fileID} in the **object** resource; and
    - **POST** /creation/import/json in the **dataImport** resource.

The file endpoint.