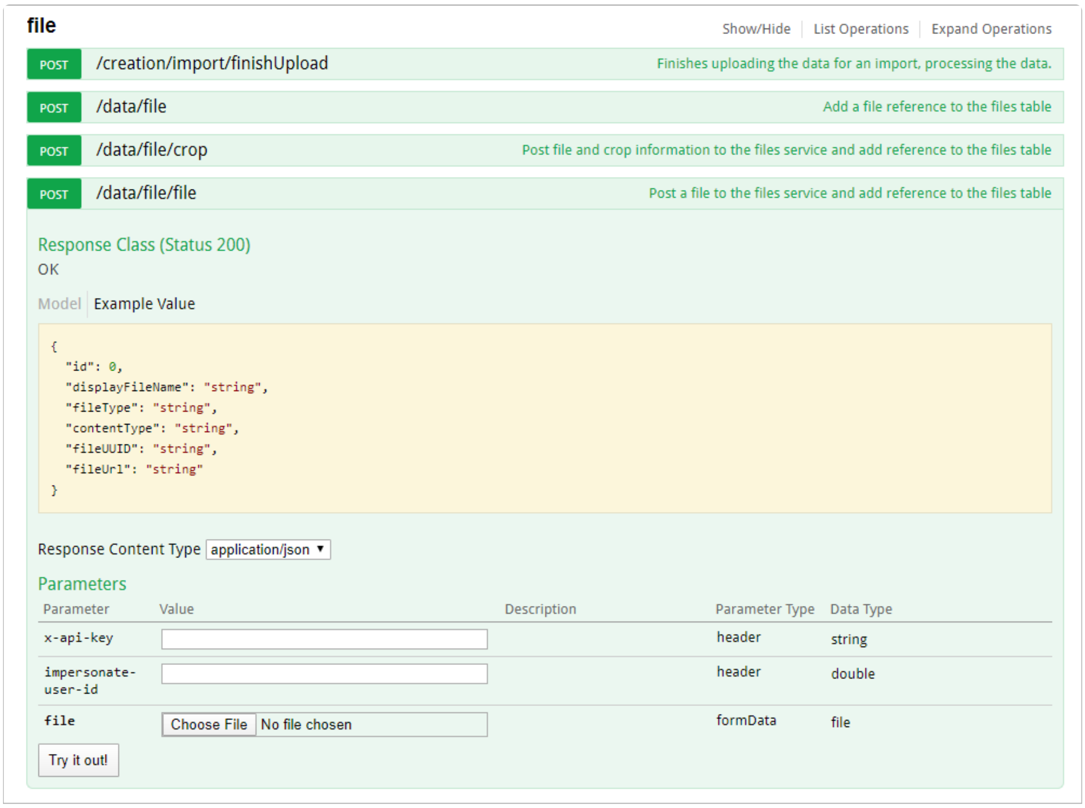
API Keys

Last Modified on 12/23/2024 3:13 pm EST

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.



file

Show/Hide | List Operations | Expand Operations

POST /creation/import/finishUpload — Finishes uploading the data for an import, processing the data.

POST /data/file — Add a file reference to the files table

POST /data/file/crop — Post file and crop information to the files service and add reference to the files table

POST /data/file/file — Post a file to the files service and add reference to the files table

Response Class (Status 200)

OK

Model | Example Value

```
{
  "id": 0,
  "displayFileName": "string",
  "fileType": "string",
  "contentType": "string",
  "fileUUID": "string",
  "fileUrl": "string"
}
```

Response Content Type application/json ▾

Parameters

Parameter	Value	Description	Parameter Type	Data Type
x-api-key			header	string
impersonate-user-id			header	double
file	Choose File No file chosen		formData	file

Try it out!

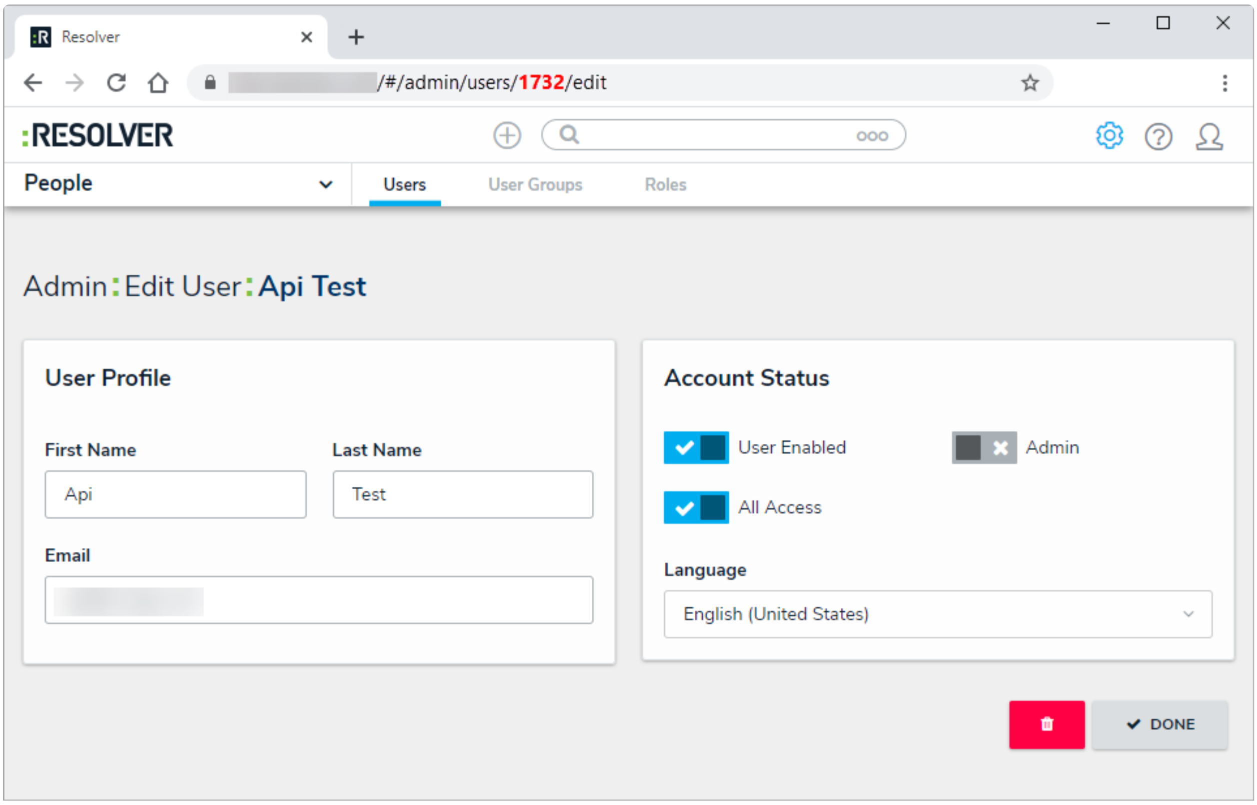
The file endpoint.

Impersonation

API keys can be used to authenticate requests in Core while impersonating another user; however, note the following:

- Impersonation can only be enabled by a member of Resolver Support at the time the key was created. Should you wish to enable impersonation, contact Resolver Support to create a new API key.
- Any user can be impersonated, provided you've obtained their user ID and the user is active in the org the API key was created for.
- Actions performed while impersonating using an API key are captured in the audit trail as "[API User's Name] impersonating [Impersonated User's Name]".
- If a user is impersonated using an external system (integration), the **Modified By** property on an object will show "[API User's Name]", but would still be captured in the audit trail as "[API User's Name] impersonating [Impersonated User's Name]".

To impersonate a user with an API key, open a supported endpoint in Swagger, enter the API key in the **x-api-key** field and the ID of the user to be impersonated in the **impersonate-user-id** field. The user ID can be obtained from the address bar of your browser after navigating to the **Edit User** page for the user (e.g., 1732).



[redacted]/#/admin/users/1732/edit

People | Users | User Groups | Roles

Admin : Edit User : Api Test

User Profile

First Name: Api

Last Name: Test

Email: [redacted]

Account Status

☑ User Enabled

☒ Admin

☑ All Access

Language: English (United States)

The Edit User page. The user ID is displayed in the address bar.

Create an API Key

Overview

API keys are used to authenticate requests to the Resolver API without entering user credentials.

User Account Requirements

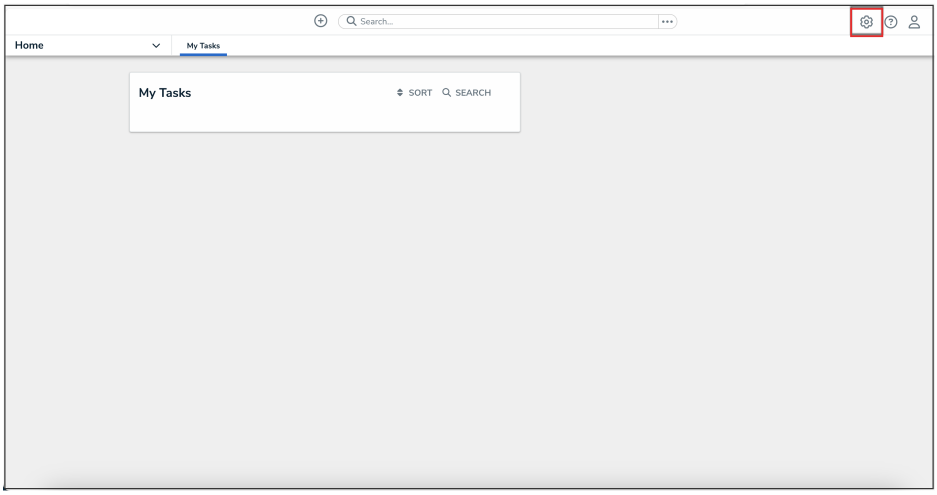
The user must have Administrator permissions to access the ***Admin Overview*** screen.

Related Information/Setup

Please refer to the API Key Overview article for more information on using API keys in Resolver.

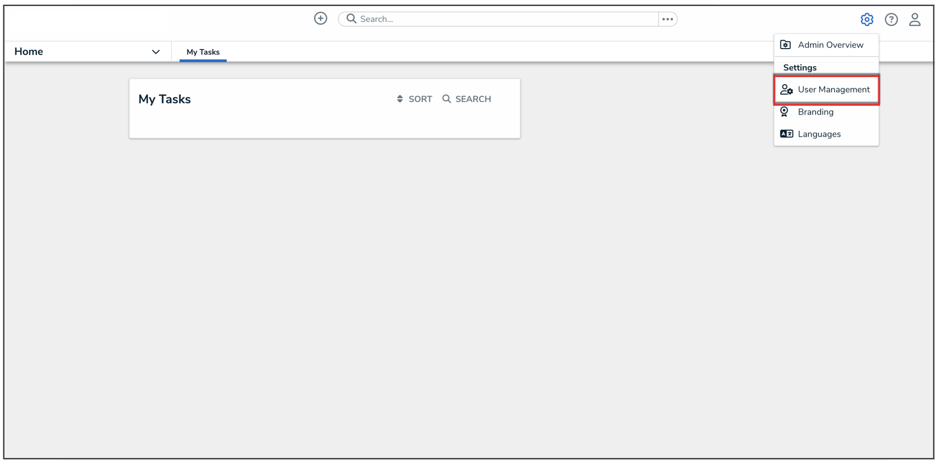
Navigation

1. From the ***Home*** screen, click the **Administration** icon.



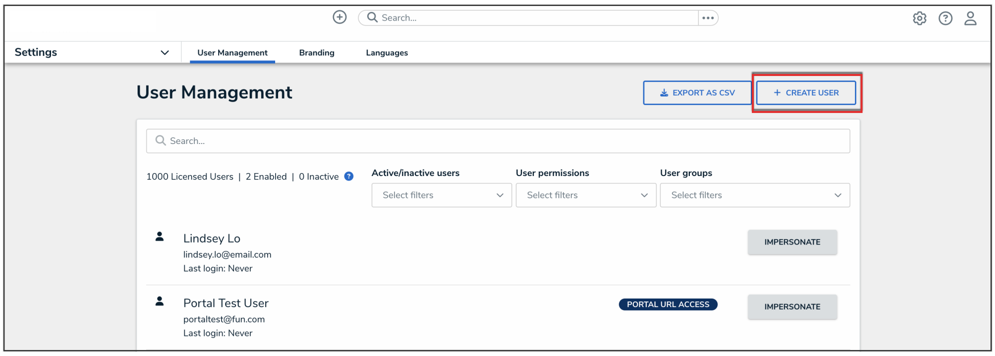
Administration Icon

2. From the **Administrator Settings** menu, click **User Management**.



Administrator Settings Menu

3. Click the **Create User** button.



1000 Licensed Users | 2 Enabled | 0 Inactive

Lindsey Lo
lindsey.lo@email.com
Last login: Never

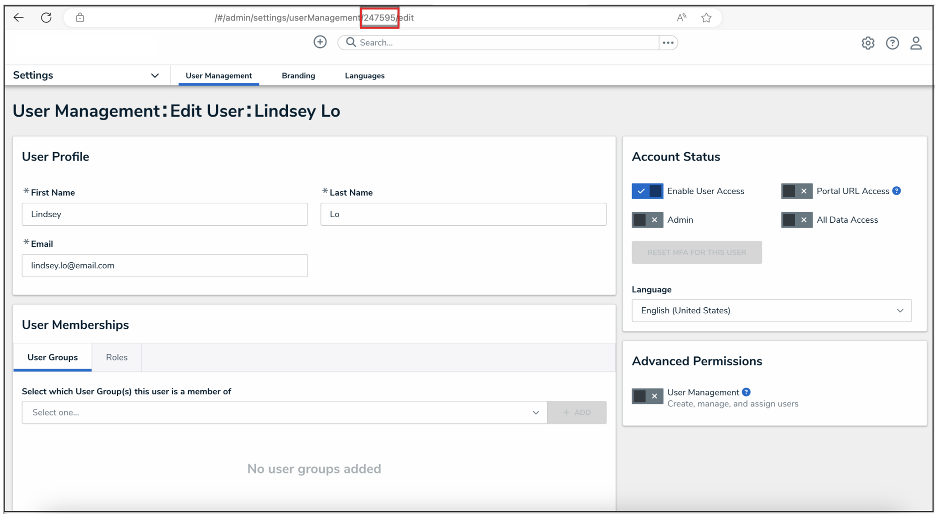
Portal Test User
portaltest@fun.com
Last login: Never

Create User Button

Creating an API Key

For added security, it's recommended that the **Admin** setting is not enabled for API users unless Administrator privileges are needed to complete the required API calls.

1. Follow the steps to create a new user.
2. From the ***Edit User*** page, record the account's internal ID from the address bar of your browser (e.g., 247595).



/#/admin/settings/userManagement/247595/edit

User Management : Edit User : Lindsey Lo

* First Name: Lindsey

* Last Name: Lo

* Email: lindsey.lo@email.com

☑ Enable User Access
☒ Portal URL Access
☒ Admin
☒ All Data Access

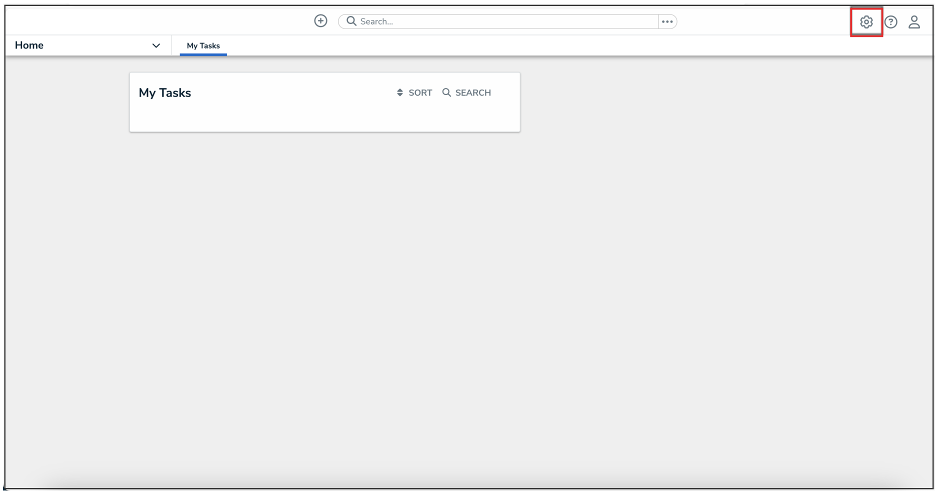
Language: English (United States)

Select which User Group(s) this user is a member of: Select one...

☒ User Management
Create, manage, and assign users

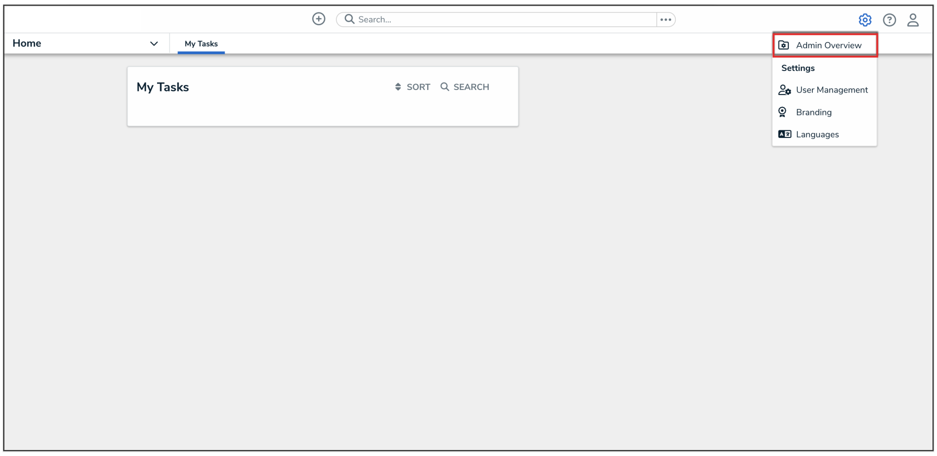
Account Internal ID

3. From the ***Home*** screen, click the **Administration** icon.



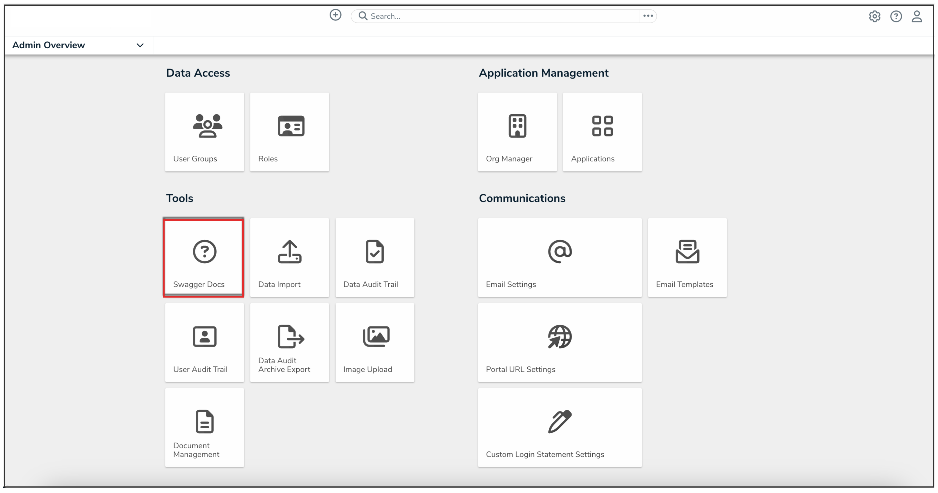
Administration Icon

4. From the **Administrator Settings** menu, click **Admin Overview**.



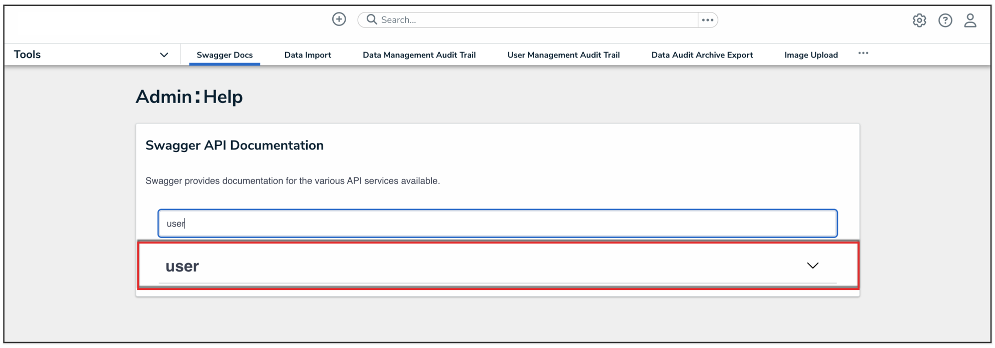
Administrator Settings Menu

5. From the ***Admin Overview*** screen, click the **Swagger Docs** tile in the **Tools** section.



Swagger Docs Tile

6. From the ***Admin: Help*** screen, enter the keyword **user** in the search text box, then click the **User** topic from the results.


Search...
Tools
Swagger Docs
Data Import
Data Management Audit Trail
User Management Audit Trail
Data Audit Archive Export
Image Upload

Admin : Help

Swagger API Documentation

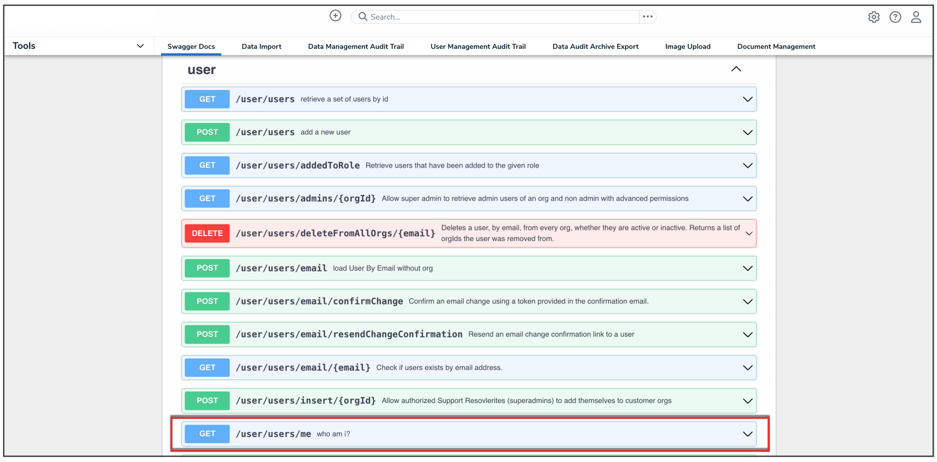
Swagger provides documentation for the various API services available.

user

user

User API Topic

7. Click the **GET /user/users/me (who am I?)** endpoint to open the parameters.


Search...
Tools
Swagger Docs
Data Import
Data Management Audit Trail
User Management Audit Trail
Data Audit Archive Export
Image Upload
Document Management
user

GET /user/users retrieve a set of users by id

POST /user/users add a new user

GET /user/users/addedToRole Retrieve users that have been added to the given role

GET /user/users/admins/{orgId} Allow super admin to retrieve admin users of an org and non admin with advanced permissions

DELETE /user/users/deleteFromAllOrgs/{email} Deletes a user, by email, from every org, whether they are active or inactive. Returns a list of orgIds the user was removed from.

POST /user/users/email load User By Email without org

POST /user/users/email/confirmChange Confirm an email change using a token provided in the confirmation email.

POST /user/users/email/resendChangeConfirmation Resend an email change confirmation link to a user

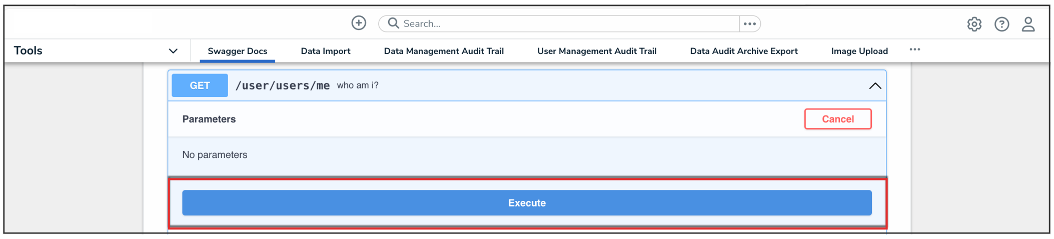
GET /user/users/email/{email} Check if users exists by email address.

POST /user/users/insert/{orgId} Allow authorized Support Resovlerites (superadmins) to add themselves to customer orgs

GET /user/users/me who am i?

API Endpoint

8. Click the **Execute** button.


Search...
Tools
Swagger Docs
Data Import
Data Management Audit Trail
User Management Audit Trail
Data Audit Archive Export
Image Upload
GET
Cancel
Execute

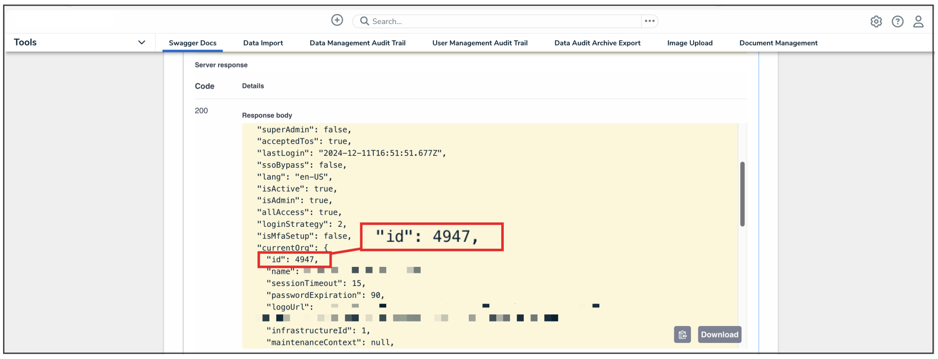
GET /user/users/me who am i?

Parameters

No parameters

Execute Button

9. Record or copy the **id** number to your clipboard from the **currentOrg** section. This is the current org's internal ID.



Server response

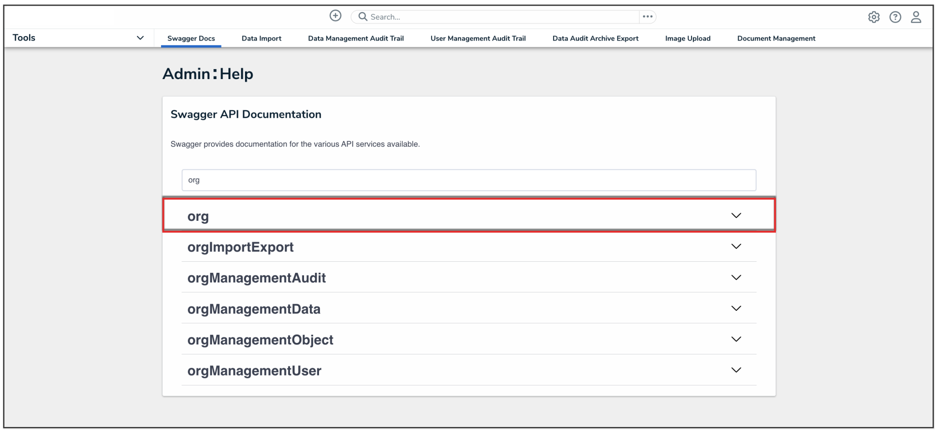
Code Details

200 Response body

```
"superAdmin": false,
"acceptedTos": true,
"lastLogin": "2024-12-11T16:51:51.677Z",
"ssoBypass": false,
"lang": "en-US",
"isActive": true,
"isAdmin": true,
"allAccess": true,
"loginStrategy": 2,
"isMfaSetup": false,
"currentOrg": {
  "id": 4947,
  "name": [redacted]
  "sessionTimeout": 15,
  "passwordExpiration": 90,
  "logoUrl": [redacted]
  "infrastructureId": 1,
  "maintenanceContext": null,
```

CurrentORG ID Value

10. Enter the keyword **org** in the search text box, then click the **Org** topic from the results.


Search...
Tools
Swagger Docs
Data Import
Data Management Audit Trail
User Management Audit Trail
Data Audit Archive Export
Image Upload
Document Management

Admin : Help

Swagger API Documentation

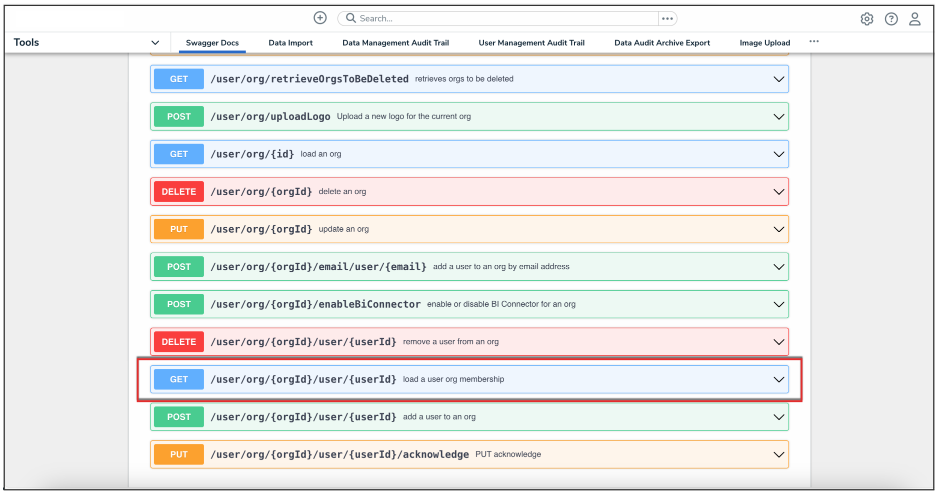
Swagger provides documentation for the various API services available.

org

- org
- orgImportExport
- orgManagementAudit
- orgManagementData
- orgManagementObject
- orgManagementUser

Org API Topic

11. Click the **GET /user/org/{orgId}/user/{userId} (load a user org membership)** endpoint to open the parameters.


Search...
Tools
Swagger Docs
Data Import
Data Management Audit Trail
User Management Audit Trail
Data Audit Archive Export
Image Upload

GET /user/org/retrieveOrgsToBeDeleted retrieves orgs to be deleted

POST /user/org/uploadLogo Upload a new logo for the current org

GET /user/org/{id} load an org

DELETE /user/org/{orgId} delete an org

PUT /user/org/{orgId} update an org

POST /user/org/{orgId}/email/user/{email} add a user to an org by email address

POST /user/org/{orgId}/enableBiConnector enable or disable BI Connector for an org

DELETE /user/org/{orgId}/user/{userId} remove a user from an org

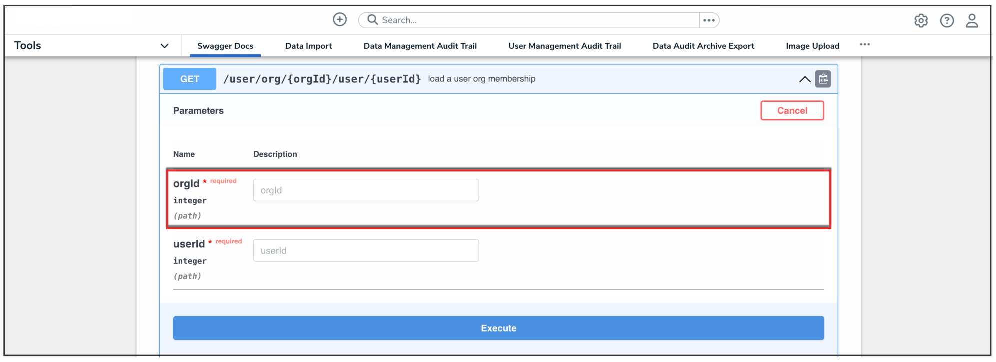
GET /user/org/{orgId}/user/{userId} load a user org membership

POST /user/org/{orgId}/user/{userId} add a user to an org

PUT /user/org/{orgId}/user/{userId}/acknowledge PUT acknowledge

API Endpoint

12. Enter the Org ID number copied during step 9 in the **orgId** field.


Search...
Tools
Swagger Docs
Data Import
Data Management Audit Trail
User Management Audit Trail
Data Audit Archive Export
Image Upload
Cancel
Execute

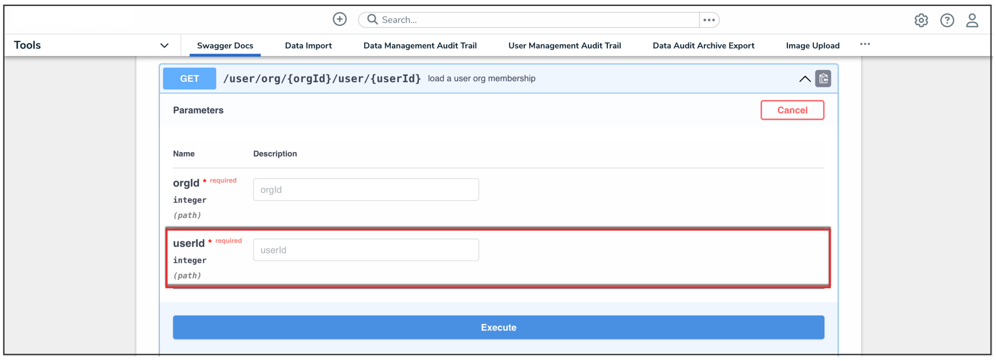
GET /user/org/{orgId}/user/{userId} load a user org membership

Parameters

Name	Description
orgId * required integer *(path)*	orgId
userId * required integer *(path)*	userId

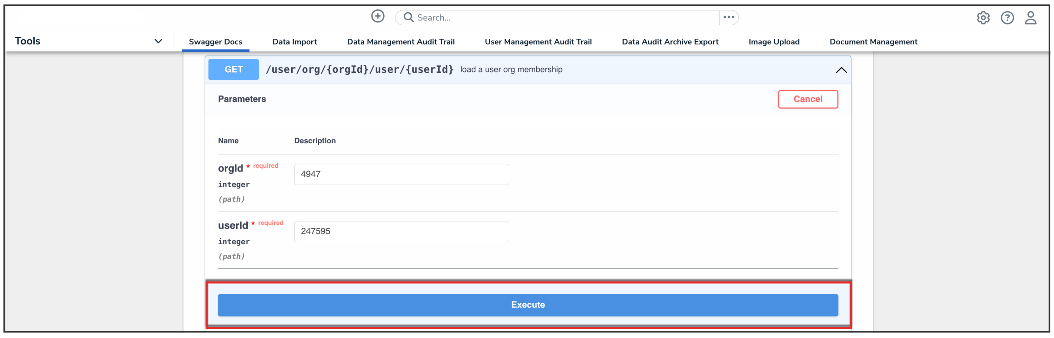
OrgID Field

13. Enter the user ID, copied during step 2 from the ***Edit User*** page, in the **userId** field.



UserID Field

14. Click the **Execute** button.

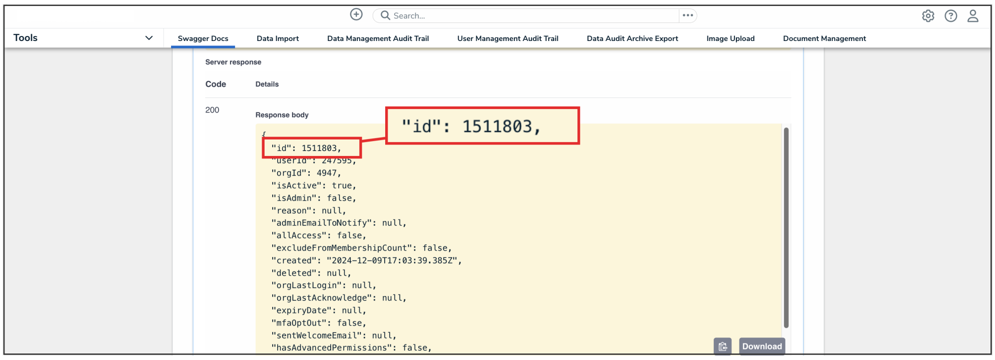


orgId: 4947

userId: 247595

Execute Button

15. From the **Response Body**, record or copy the **id** number to your clipboard. This is the user's org membership ID number.

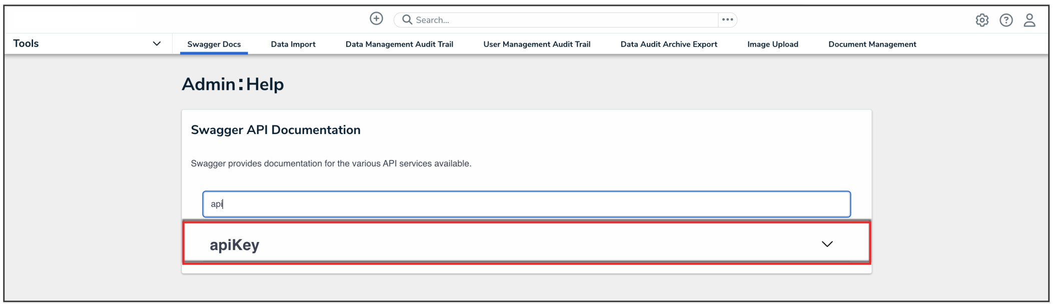


```
{
  "id": 1511803,
  "userId": 247595,
  "orgId": 4947,
  "isActive": true,
  "isAdmin": false,
  "reason": null,
  "adminEmailToNotify": null,
  "allAccess": false,
  "excludeFromMembershipCount": false,
  "created": "2024-12-09T17:03:39.385Z",
  "deleted": null,
  "orgLastLogin": null,
  "orgLastAcknowledge": null,
  "expiryDate": null,
  "mfaOptOut": false,
  "sentWelcomeEmail": null,
  "hasAdvancedPermissions": false,
```

"id": 1511803,

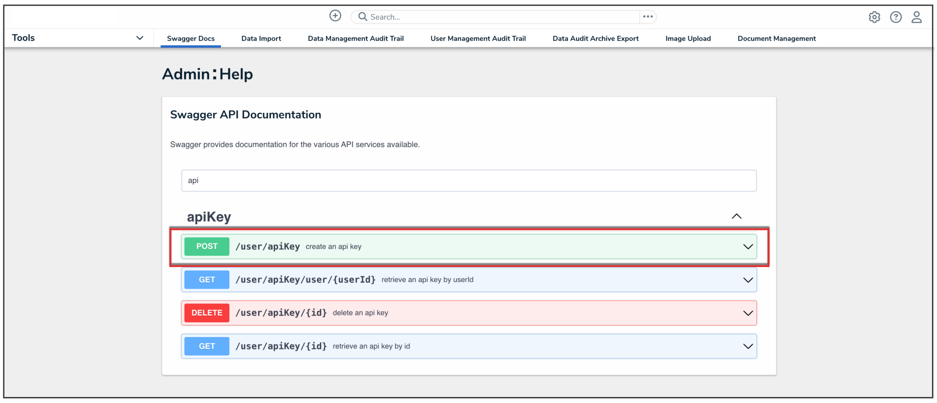
ID Value

16. Enter the keyword **apiKey** in the search text box, then click the **apiKey** topic from the results.


Search...
Tools
Swagger Docs
Data Import
Data Management Audit Trail
User Management Audit Trail
Data Audit Archive Export
Image Upload
Document Management
Admin: Help
Swagger API Documentation
Swagger provides documentation for the various API services available.
api
apiKey

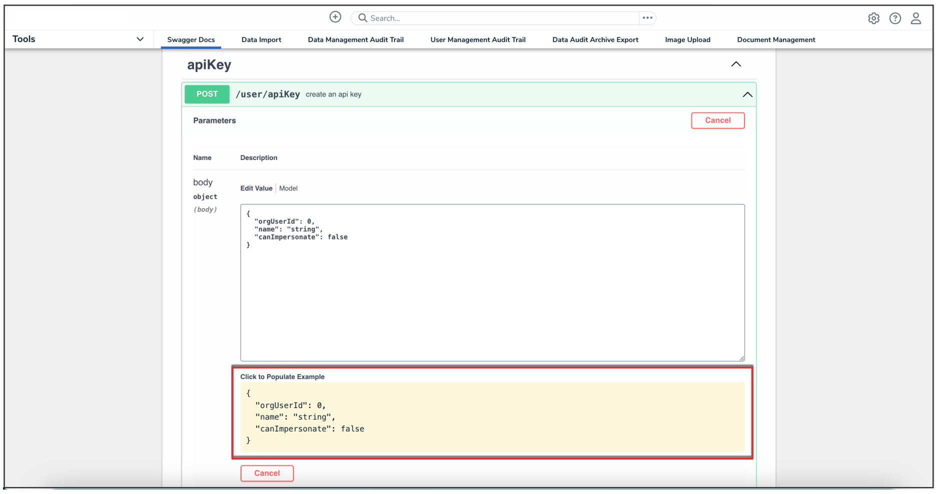
APIKey Topic

17. Click the **POST /user/apiKey (create an api key)** endpoint to open the parameters.


Search...
Tools
Swagger Docs
Data Import
Data Management Audit Trail
User Management Audit Trail
Data Audit Archive Export
Image Upload
Document Management
Admin : Help
Swagger API Documentation
Swagger provides documentation for the various API services available.
api
apiKey
POST /user/apiKey create an api key
GET /user/apiKey/user/{userId} retrieve an api key by userId
DELETE /user/apiKey/{id} delete an api key
GET /user/apiKey/{id} retrieve an api key by id

API Endpoint

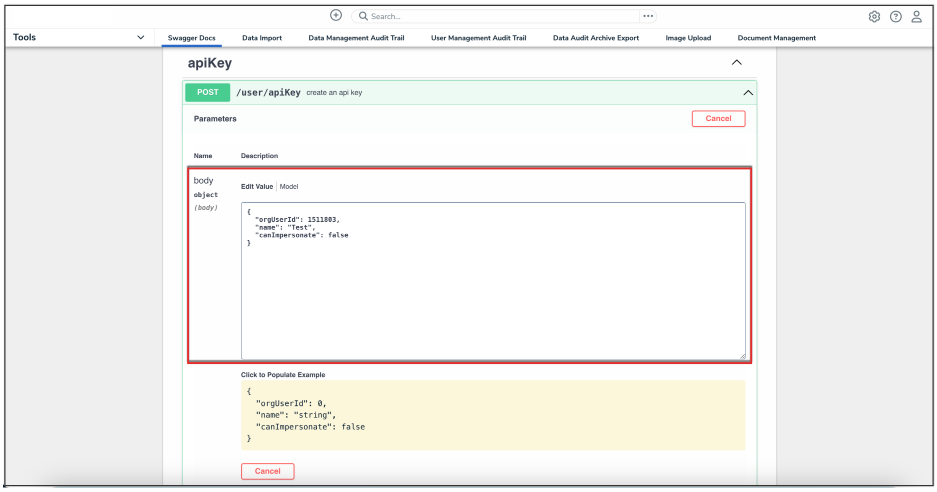
18. In the **Parameters** section, click the **Click to Populate Example** box to populate the template in the **body** text box.



```
{
  "orgUserId": 0,
  "name": "string",
  "canImpersonate": false
}
```

Click to Populate Example Box

19. In the **body** text box, delete the **0** in the **orgUserId** attribute, then enter the user's org membership ID number, obtained in step 15. Enter a descriptive name for the API key in the **name** attribute.

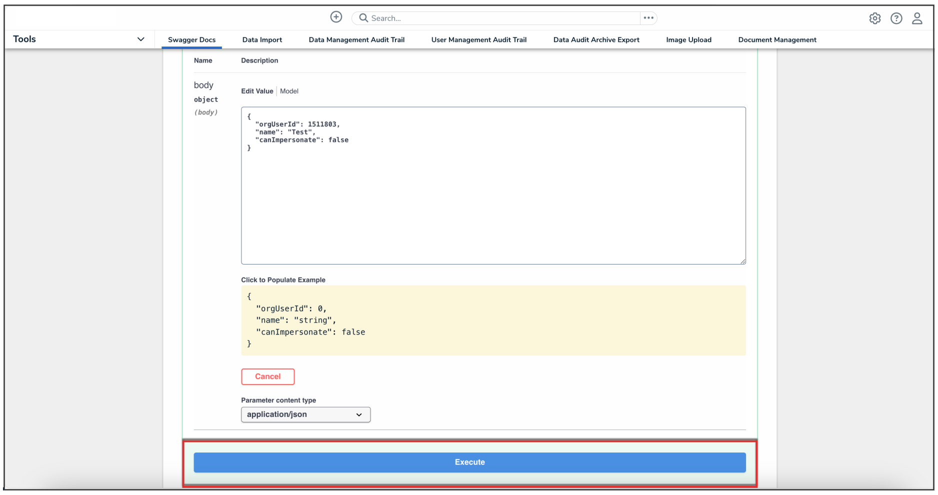


```
{
    "orgUserId": 1511803,
    "name": "Test",
    "canImpersonate": false
}
```

```
{
  "orgUserId": 0,
  "name": "string",
  "canImpersonate": false
}
```

Body Text Box

20. Click the **Execute** button.



```
{
    "orgUserId": 1511803,
    "name": "Test",
    "canImpersonate": false
}
```

```
{
  "orgUserId": 0,
  "name": "string",
  "canImpersonate": false
}
```

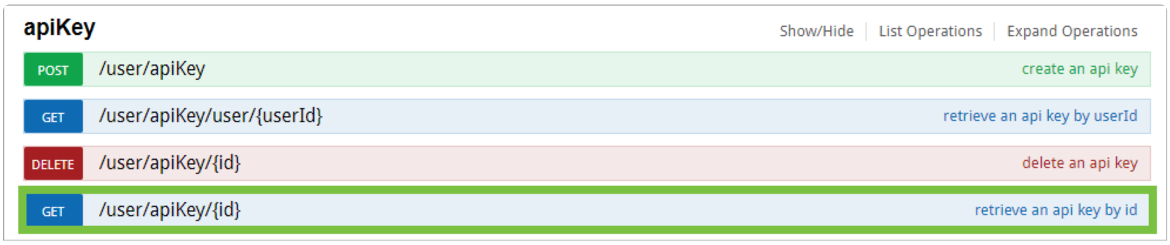
Execute Button

21. Copy the **apiKey** from the **Response Body** and store it for safekeeping. For security purposes, once an API key is generated, it cannot be retrieved. If you misplace an API key, a new key must be generated.

Delete an API Key

To delete an API key:

1. Log in as an admin and select the appropriate org, if required.
2. Click the ⚙ icon in the top bar **> Swagger Docs** in the **Tools** section.
3. Click any resource to open the Swagger interface in a new tab.
4. Click the **apiKey** service to display its endpoints.
5. Click **GET /user/apiKey/{id} (retrieve an api key by id)** to expand it.



apiKey   Show/Hide | List Operations | Expand Operations

POST /user/apiKey   create an api key

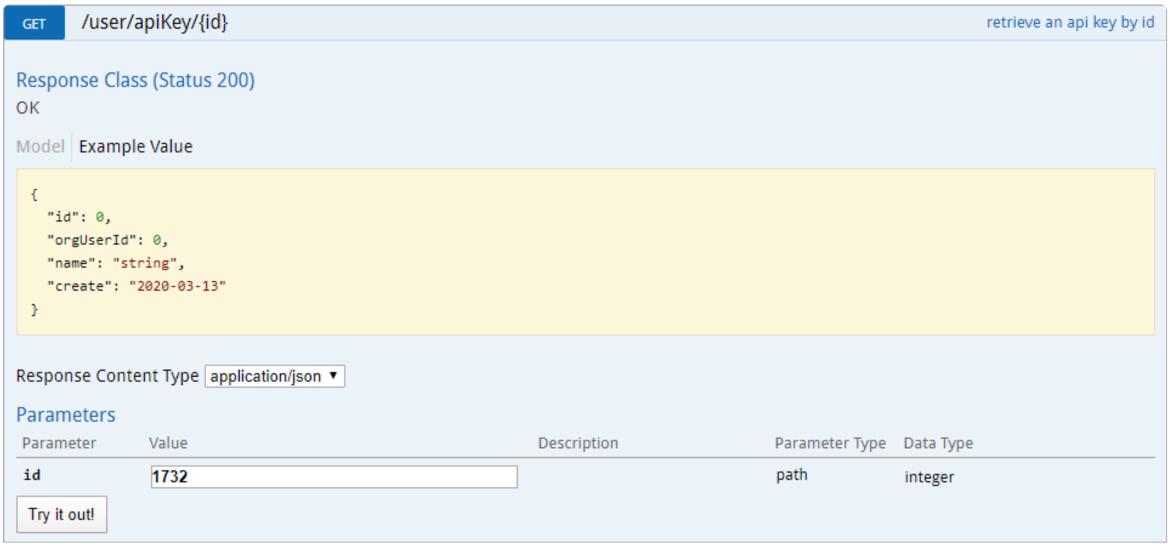
GET /user/apiKey/user/{userId}   retrieve an api key by userId

DELETE /user/apiKey/{id}   delete an api key

GET /user/apiKey/{id}   retrieve an api key by id

The apiKey service.

6. Enter the user ID of the account the API key was created under in the **id** field. The user ID can be obtained from the address bar of your browser after navigating to the **Edit User** page for the user.



GET /user/apiKey/{id}   retrieve an api key by id

Response Class (Status 200)

OK

Model | Example Value

```
{
  "id": 0,
  "orgUserId": 0,
  "name": "string",
  "create": "2020-03-13"
}
```

Response Content Type application/json ▾

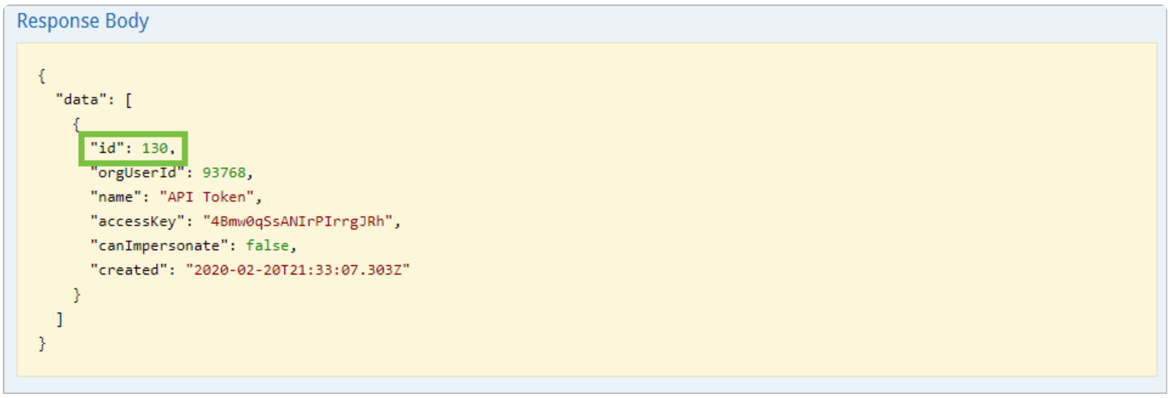
Parameters

Parameter	Value	Description	Parameter Type	Data Type
id	1732		path	integer

Try it out!

The GET /user/apiKey/{id} (retrieve an api key by id) endpoint.

7. Click **Try it out!**
8. Copy the **id** from the **Response Body** to your clipboard. This is the internal ID for the API key.

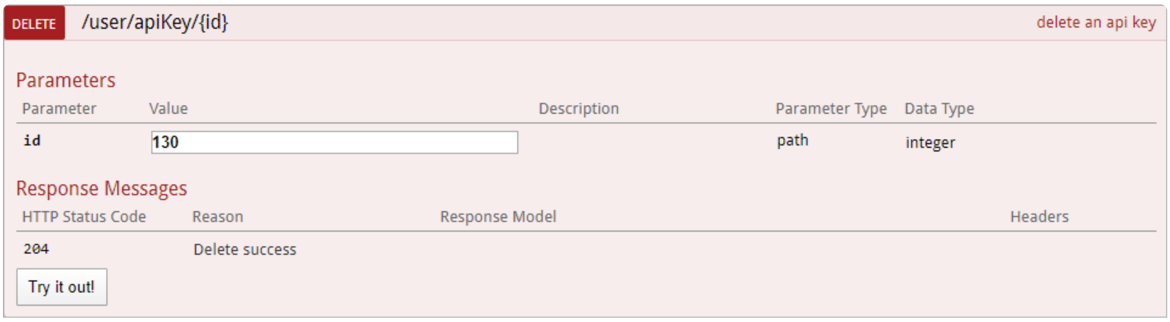


Response Body

```
{
  "data": [
    {
      "id": 130,
      "orgUserId": 93768,
      "name": "API Token",
      "accessKey": "4Bmw0qSsANIrPIrrgJRh",
      "canImpersonate": false,
      "created": "2020-02-20T21:33:07.303Z"
    }
  ]
}
```

*The id in the **Response Body**.*

9. Click **DELETE /user/apiKey/{id} (delete an api key)** to expand it.
10. Paste the internal API key ID obtained from step 8 above in the **id** field.



DELETE /user/apiKey/{id}

delete an api key

Parameters

Parameter	Value	Description	Parameter Type	Data Type
id	130		path	integer

Response Messages

HTTP Status Code	Reason	Response Model	Headers
204	Delete success		

The DELETE /user/apiKey/{id} (delete an api key) endpoint.

11. Click **Try it out!** to delete the API key.

IP Token Validation

IP token validation protects the Core API (Swagger) from unauthorized users and can be used in conjunction with IP authorization to manage organizational access. The token validation process accomplishes this by periodically validating the IP associated with the token. If there is any change to the IP during the session, the user will be logged out and asked to log in again.

IP token validation can be used with one of the following options:

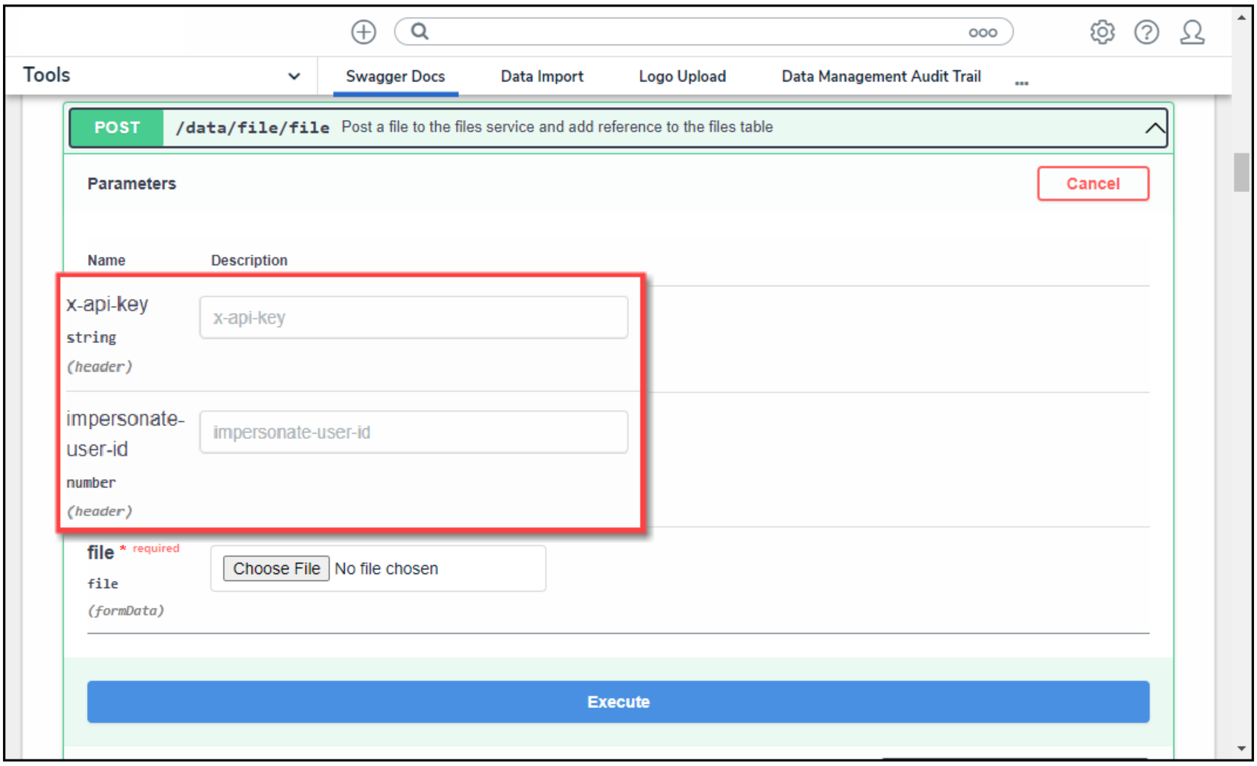
- **off:** No IP token validation is performed for any authentication requests. This is the default setting for IP token validation.
- **on:** IP token validation is performed for all SSO and basic API access requests.

The above options can be enabled and disabled by Resolver Support. See the IP Authorization Logins article for login functionality when this feature is enabled.

Make Calls

To use an API key in the Swagger interface:

1. Log in as an admin and select the appropriate org, if required.
2. Navigate to **Admin > Swagger Docs**.
3. Click the resource from the list to open the Swagger interface in a new tab.
4. Expand a supported endpoint.
5. Enter the API key in the **x-api-key** field to authenticate the call.
6. **Optional:** If impersonation is enabled, enter the ID of the user who will be impersonated. Impersonation can only be enabled by a member of Resolver Support. See Impersonation with an API Key for more details.



*The POST /data/file/file endpoint in the **file** service*

7. Complete the remainder of the fields as required.

Example

```
curl -X POST --header 'Content-Type: multipart/form-data' --header 'Accept: application/json' --header 'x-api-key: YOUR_A
```