# Impersonation with an API Key

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

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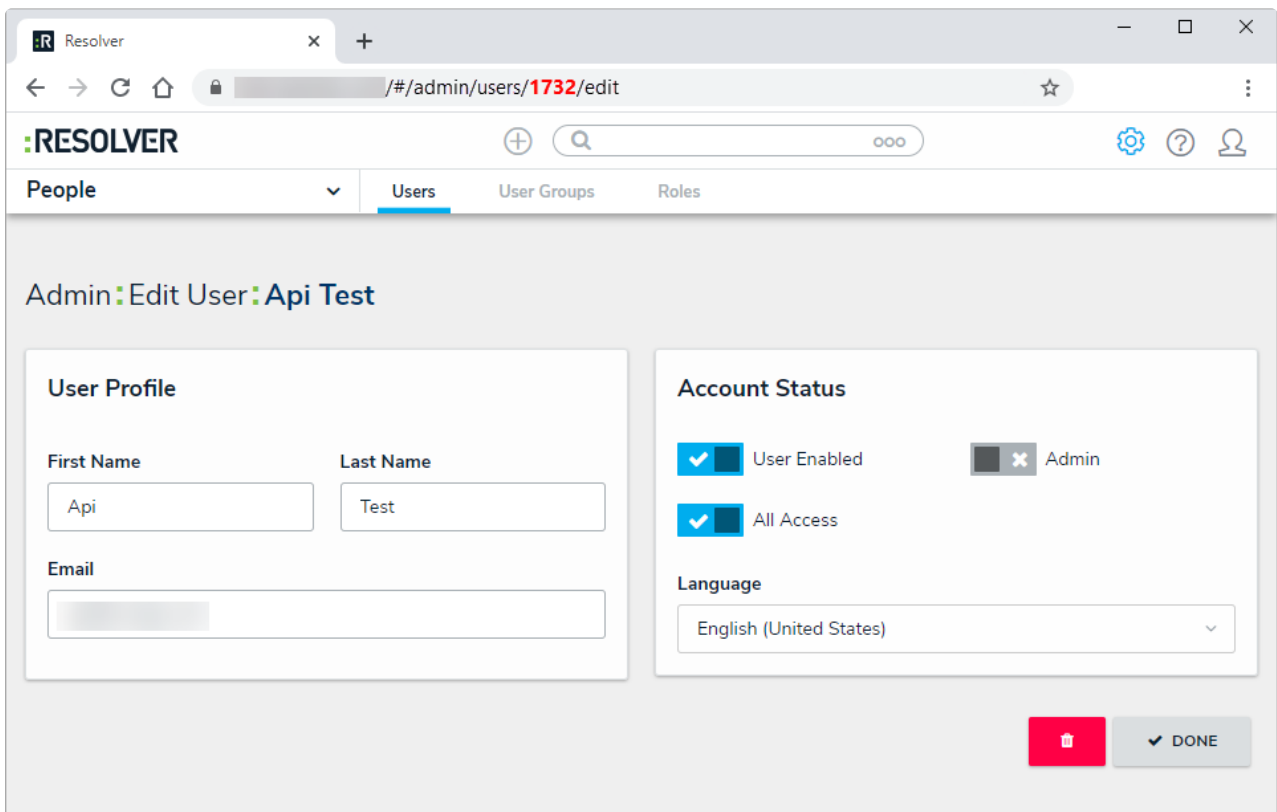
The Edit User page. The user ID is displayed in the address bar.