

# 4.3. User - Manage user secrets [canceled]

<b>Id</b>	4.3.
<b>Description</b>	<p>As a <b>Generic User</b></p> <p>I want to be able to manage my secrets linked to the chosen authentication mechanism and to revoke consents given to external applications,</p> <p>So that I can grant and revoke access given to external applications to my account</p>
<b>Priority</b>	<b>High</b>
<b>Actors</b>	User
<b>API Calls</b>	N/A
<b>Linked Processes</b>	
<b>Status</b>	<b>Canceled</b> - Each application will receive a dedicated user with the appropriate role and a dedicated access token

## Preconditions

1. The **User** must be authenticated.

## Postconditions

1. The System returns a list of external application to which the user has granted access.
2. The system updates the external application secrets / information as requested by the user.
3. If the user choses to revoke the external application's permissions, the system deletes that external application's credentials and the application can no longer access the system on behalf of the user.

## Main flow

1. The **User** retrieves the list of external applications to which he has granted access (GET).
2. The user performs the updates needed to the external applications grants (e.g. update secrets, change name, ...) (PUT)
3. If needed the user can revoke the access granted to an external application (DELETE)
4. The system applies the instructions given by the user.

## Exceptions

### [400 Bad Request] Invalid input:

If mandatory fields are missing or invalid, the system returns an error message.

### [500 Internal Server Error] System Error

If the system fails to save changes due to an internal error, it displays an appropriate message and logs the error for further investigation.

---

Revision #5

Created 15 October 2025 04:32:02 by Sergio Sousa

Updated 15 October 2025 05:03:37 by Sergio Sousa