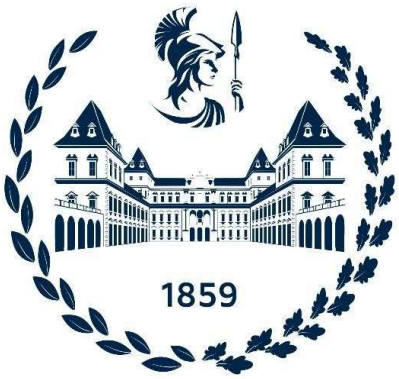
POLITECNICO DI TORINO

Master's degree in computer science

System and Device Programming Special Project
in collaboration with

AROL S.P.A.



An IoT Application on Capping Devices

DOCUMENTATION

Supervisors:

Prof. Stefano Quer

Ing. Mario Deda

Team Members:

Nicolò Caradonna

Roberto Ferrareis

Giuseppe Lisena

Academic Year 2022/2023

1. Introduction

This project is aimed to enhance the current web application designed for AROL, specifically focusing on the integration of bottling machineries. The current implementation of the application is primarily focused on user management for partner companies that have purchased machinery from AROL. It includes permissions management related to the operations these users can perform on the associated machinery.

The work addressed in this project is a proposed extension that aims to widen the scope to incorporate AROL users responsible for managing partner companies. This expansion necessitates accommodating not only the machineries owned by these partner companies but also the operations that both the partner companies and AROL users can perform within the web application. The goal is to create a more complete and inclusive platform that addresses the needs of both partner companies and AROL users, providing a unified interface and access methods for efficient management and operation of bottling machineries.

---

2. Existing Work

The foundational application upon which development began was designed with a limited set of operations primarily centered around company users, excluding AROL (specific details of AROL users are not provided). Within this system, three distinct user roles were established:

1. **Administrator**
    - *Role*: holds the highest level of authority within the company.
    - *Permissions*: granted access to every entity, including machinery and other user profiles.
    - *Responsibilities*: manages the entire company, overseeing all aspects of machinery and user administration.
2. **Manager**
    - *Role*: acts as a delegate for the Administrator, possessing similar permissions.
    - *Permissions*: limited to a designated subset of machineries assigned by the Administrator.
    - Restrictions: while able to modify user profiles, Managers do not have the authority to delete users.
    - *Responsibilities*: supports the Administrator in overseeing and managing a specific set of machineries.
3. **Worker**
    - *Role*: occupies the lowest tier in the hierarchy.
    - *Permissions*: limited to specific actions within machineries, such as interacting with dashboards and documents.
    - *Restrictions*: cannot manage other users.
    - *Responsibilities*: primarily involved in day-to-day operations related to machinery, utilizing dashboards and documents for task execution.

The central focus of this application revolves around the core entity of machinery. Each machinery unit is accompanied by dashboards containing sensors for monitoring and documents for essential information.

3. Project Extension

3.1. Overview

The project requirements include the following mandatory features to be implemented:

- New user roles for the AROL superusers: this will define what the user will be able to access
- User management features (user must be part of a company):
    - Create new user account
    - Update existing user account
    - Delete and disabled existing user account
    - Modify user account permissions
    - Password reset + random password generator option
    - User filtering and search
- Machinery management features (machinery must be assigned to a company):
    - Create/update/delete machinery with all its specifications (including sensors)
    - Machinery templates support (e.g., a certain machinery model)
    - Create/update/delete machinery dashboard templates
    - Manage machinery access permissions
    - Machinery filtering and search

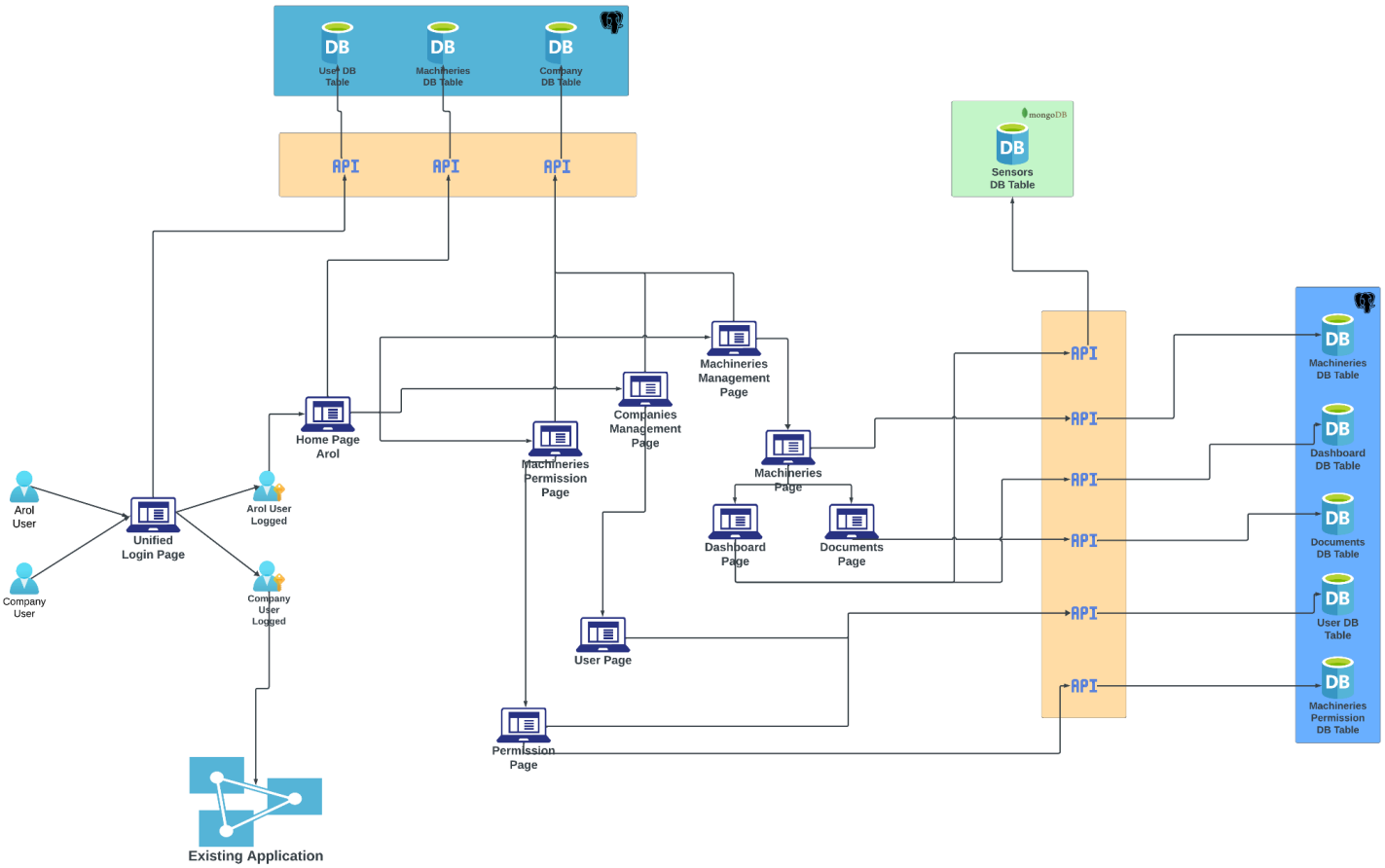
Plus some additional optional features have been implemented:

- Module for creation and management of a new company
- Management for a temporary user
- File privacy strategy
- File ownership update on deletion

3.2. Technological Stack

- **Programming Language**: Typescript
- **Framework**: React.js
- **Database**: MongoDB (for sensor data), PostgreSQL (for access to web application data)
- **Backend**: Express.js (Node.js)
- **Frontend**: Chakra UI, React Grid Layout

3.3. System Design Diagram



4. New roles for AROL users

New AROL roles have been defined and managed in both the web application and database. In order to introduce minimal changes into the database schema the AROL users are identified with a company ID set to 0. This solution made the development much easier and consistent with the concept of the company.

1. **Chief**
    - *Role*: this role encompasses the management of all aspects within the system.
    - *Permissions*: this user has all permissions on all users, machineries and companies managed by the application.
    - *Responsibilities*: manages all entities of the web application, for all companies and within AROL.
2. **Supervisor**
    - *Role*: similar to a Chief, a Supervisor possesses the ability to execute various operations but is restricted to a limited set of resources.
    - *Permissions*: this user has all the permissions on the user and companies.
    - *Restrictions*: manages only machinery on which has permissions. These permissions are given by a Chief user.
    - *Responsibilities*: manages all the users and a subset of the machineries.
3. **Officer**
    - *Role*: a user with knowledge on the system's resources but does not engage in operational management.
    - *Permissions*: this user has only read permissions on a limited set of machineries.
    - *Restrictions*: this user does not have permission to handle machineries.
    - *Responsibilities*: only manages documents, dashboards of machineries to which has access.

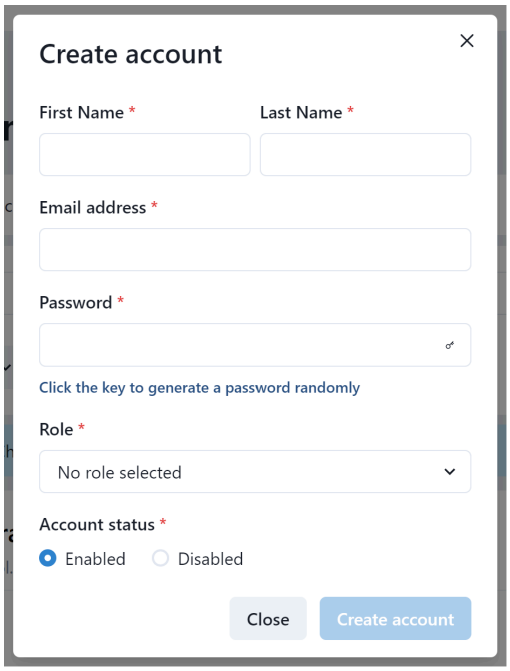
ROLES	MACHINERY							
	Dashboards				Documents			
	C	R	U	D	C	R	U	D
CHIEF	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SUPERV.	Yes*	Yes*	Yes*	Yes*	Yes*	Yes*	Yes*	Yes*
OFFICER	Yes*	Yes*	Yes*	Yes*	Yes*	Yes*	Yes*	Yes*

C: Create, R: Retrieve, U: Update, D: Delete

* if has permissions

5. User Management Features

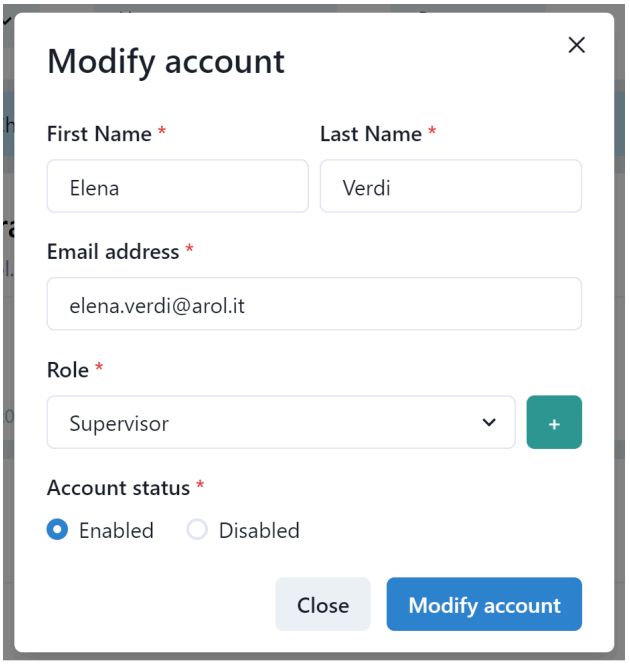
5.1. Creation a new user account



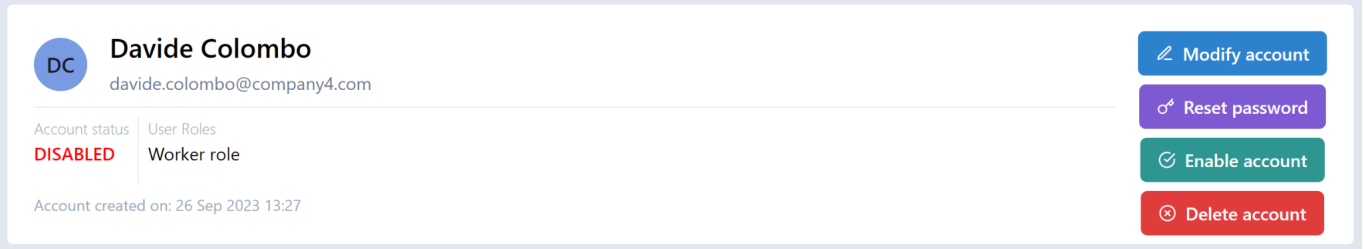
A new module has been developed with the primary objective of facilitating the creation of new users within the AROL system. This module, which previously existed, has undergone an extension in order to adapt specifically to the creation of new AROL users.
The reworked module now offers the functionality to assign one or more roles to the newly created AROL users. This enhancement provides users with the flexibility to select and define the roles that best align with their organizational requirements.
This module is accessible, in addition to locations in the base application, by AROL when a related user accesses the company management page or when managing machinery permissions.

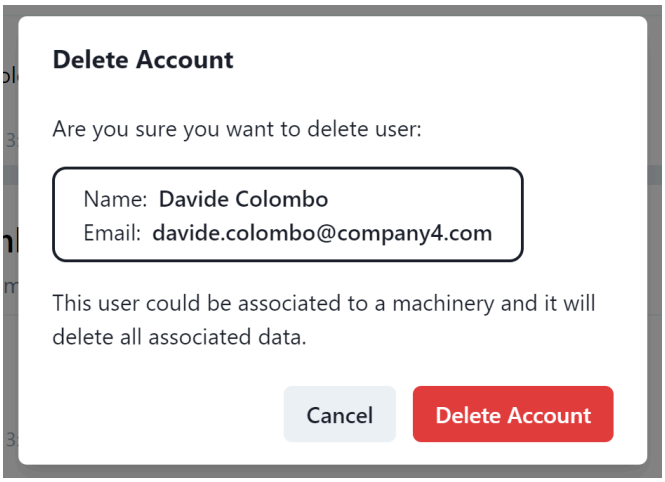
5.2. Update of an existing user account

This functionality is managed through the same module introduced in the preceding feature. However, it has been modified to enable the updating of individual user information, with the exception of password modifications. The handling of password changes has been segregated into a distinct feature and corresponding modules. This separation ensures a more organized and secure approach to user data management, allowing for focused attention on password-related updates while maintaining the versatility of the primary user information module for other modifications.



5.3. Deletion and disable of an existing user account

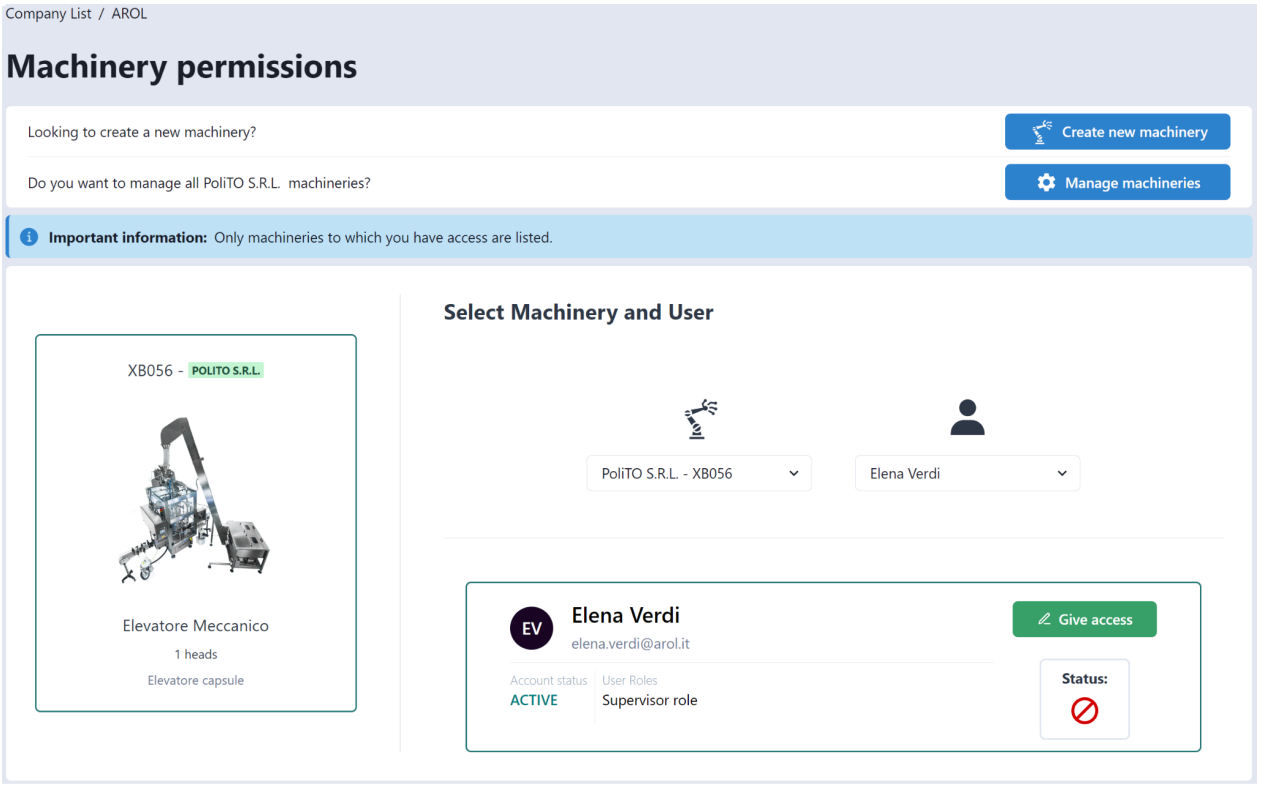




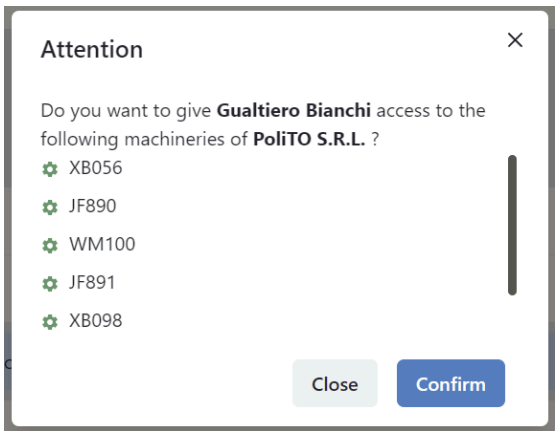
This feature was initially part of the core application and has now been expanded to accommodate AROL users in the new system. In this enhanced functionality, a two-step process is implemented for user management. Initially, users must be disabled before they can be permanently deleted. This strategic approach ensures that users are placed in a status that allows for careful consideration, with the option to either confirm the deletion or revert the action by enabling the account.

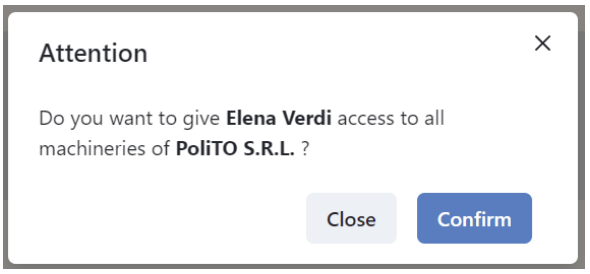
The actual deletion process is executed by database triggers, which comprehensively manage the removal of all user-related information. This includes permissions on machineries, ensuring that access rights are revoked, and ownership of documents is seamlessly transferred to another designated user. By incorporating these measures, the system ensures a secure user deletion process, maintaining data integrity and accountability throughout the operation.

5.4. Modification of user account permissions



A new permission module has been introduced to streamline permission management specifically for AROL users. Notably, the relationship between AROL users and machinery permissions adopts a monolithic structure compared to the more intricate, fine-grained permission systems present in the base application. This means that an AROL user, when granted permissions on a machine, possesses comprehensive management capabilities. However, certain restrictions are in place to cater to the nuanced responsibilities of different user roles. For example, an officer with permissions to modify machinery dashboards and documents cannot alter the sensors installed on the machine.

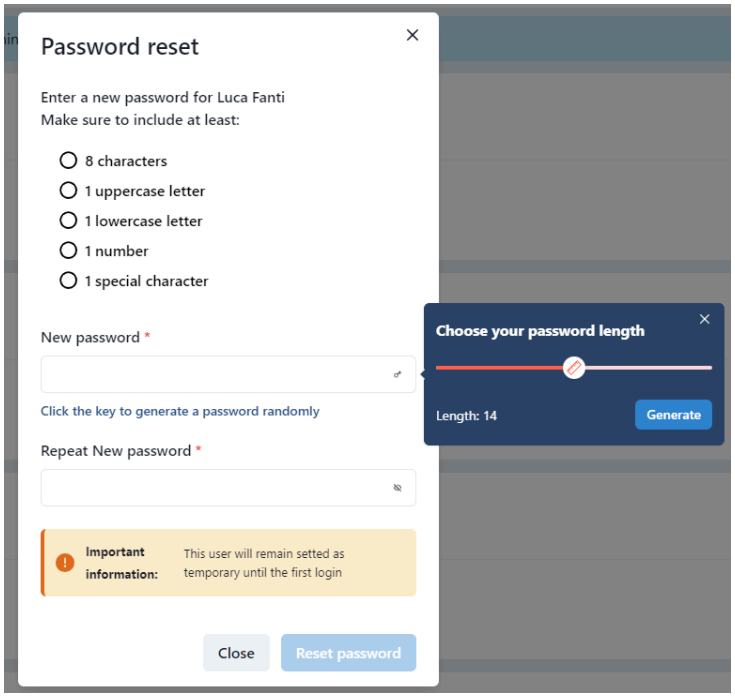




Additionally, the system allows for the assignment of permissions to all machinery within a company to a selected user based on the permissions owned by the logged user. It establishes a hierarchical permission structure that maintains security and operational integrity.

To ensure a secure and controlled environment, certain restrictions are imposed on the permission systems. A logged user, based on their rank, is restricted from modifying the permissions of users with a higher or equal rank. This approach safeguards the integrity of the permission hierarchy.

5.5. Password reset + random password generator option



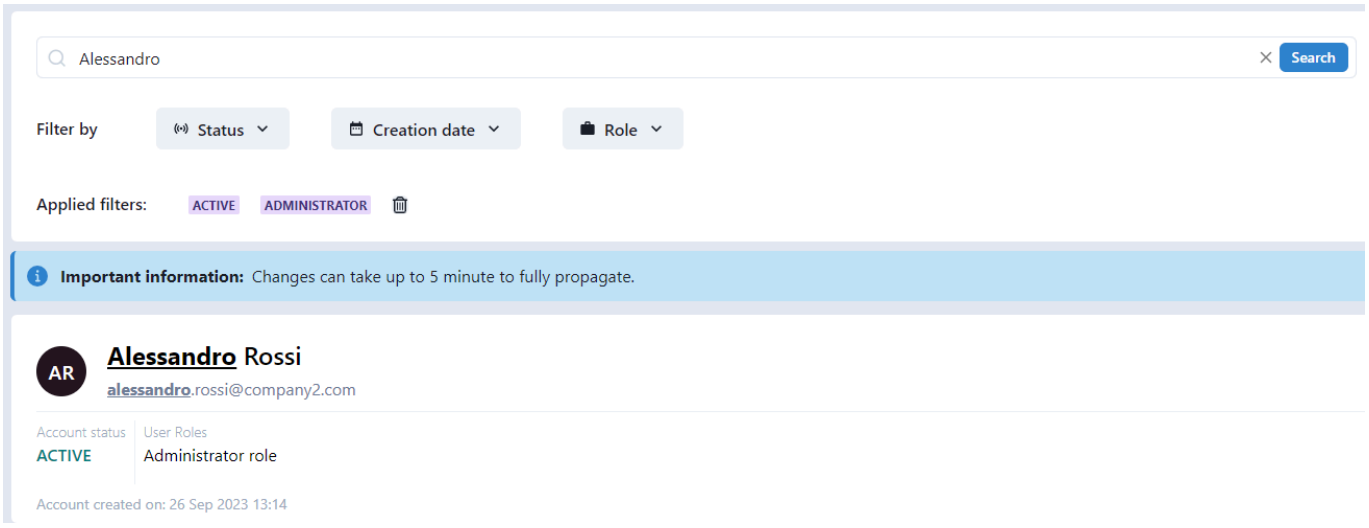
The password reset functionality has been separated from the user update module and established as a distinct module within the user management system. Access to this module is restricted, requiring the logged user to possess user management permissions, specifically as an Administrator (within a company), Chief, or Supervisor. Notably, the password reset option is disabled if the users involved share the same rank.

When initiating a password change, the system provides graphical prompts that offer security and complexity advisories.

While an 8-character constraint is mandatory for testing purposes, other recommendations are presented graphically but remain non-mandatory. This approach ensures flexibility while encouraging users to adhere to best practices for password security.

Moreover, a new password generator module has been developed to automate the creation of secure passwords of user-defined lengths. This component is utilized during password resets or when generating initial passwords for new user accounts. By incorporating this feature, the system enhances security measures and simplifies the process of creating robust passwords, contributing to a more secure user authentication environment.

5.6. User filtering and search

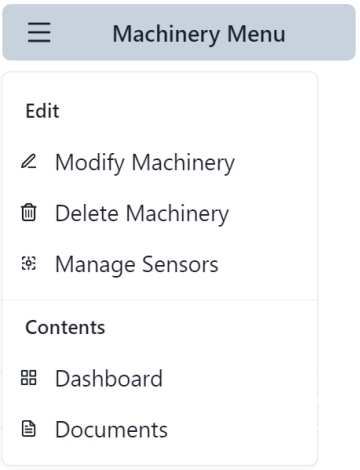


A filtering and search component for users has been developed with the specific purpose of merging both user information searches using a dedicated search bar and the application of purpose-designed filters. The filters implemented in this user module are as follows:

1. Status: This filter distinguishes between enabled and disabled users based on a designated flag, allowing users to be easily sorted based on their active or inactive status.
2. Creation Date: Users can be filtered based on their creation date, with the option to set specific date bounds. If bounds are defined, the system filters out all users created before the lower bound or after the upper bound. If no bounds are set, all users not created within the specified date range are filtered out.
3. Role: Users can be filtered based on their roles, with the flexibility to select multiple roles simultaneously.

Given that this component is associated with user visualization, it is accessible exclusively to logged-in users who possess management permissions on users. Specifically, users with roles such as Administrator, Manager, Chief, and Supervisor have the requisite permissions to access and utilize this component, ensuring a controlled and secure user management environment.

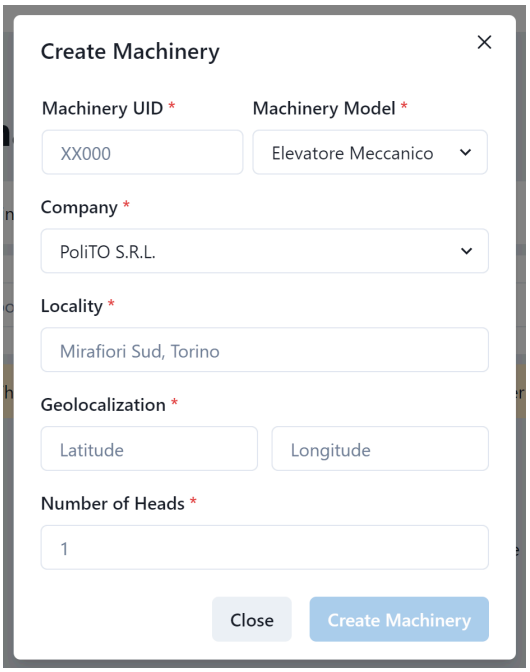
6. Machinery Management Features



Each machinery has its own menu window that can be opened to perform different kinds of operations.

6.1. Creation, update and deletion operations for machinery with all its specifications (including sensors)

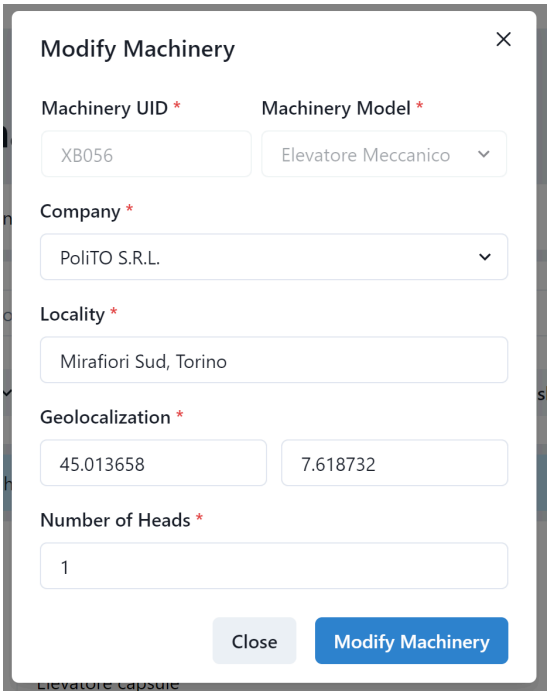
6.1.1. Creation of a machinery



The machinery creation module is accessible both through the machinery management component of each company and the AROL permissions management component. When accessed from the machinery management component of a company, the company value is automatically set to the corresponding company, ensuring proper association.
To create a new machinery entry, users need to input a set of mandatory fields, as depicted in the accompanying image. The unique identifier for each machinery entry is its Machinery UID.
This design allows for flexibility in accessing the machinery creation functionality from different modules, ensuring a seamless user experience whether managing machinery within a specific company or configuring permissions within the AROL system. The mandatory fields guarantee essential information is provided during the creation process contributing to accurate and comprehensive machinery records.
This feature is only accessible by Chief and Supervisor users.

6.1.2. Update of a machinery

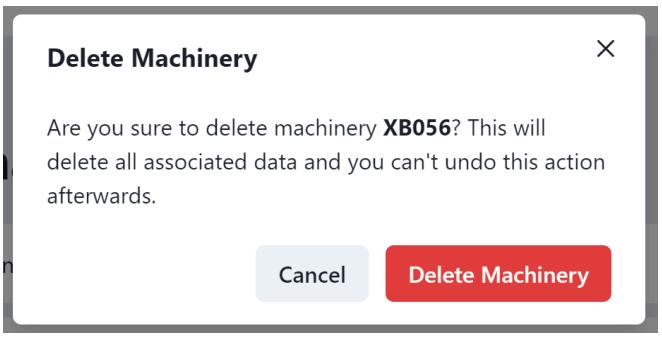
The machinery update module closely resembles the creation module, utilizing the same graphical component. In the provided image, each field associated with a machinery entry is editable, allowing for comprehensive updates. Notably, the machinery can also be reassigned to another company, facilitating efficient reuse of machinery assets.



However, certain fields have restrictions on modification. Specifically, the Machinery UID and Machinery Model fields must remain immutable. The Machinery UID serves as a unique identifier, and its unalterable nature ensures data integrity. Similarly, the machinery model is fixed, as the technical aspects of a machinery design are intricately linked to its model and cannot be changed.

Access to this update feature is restricted to users with permissions, specifically AROL Chief and Supervisor roles. This limited accessibility ensures that only authorized users can modify machinery details, contributing to data security and system integrity.

6.1.3. Deletion of a machinery

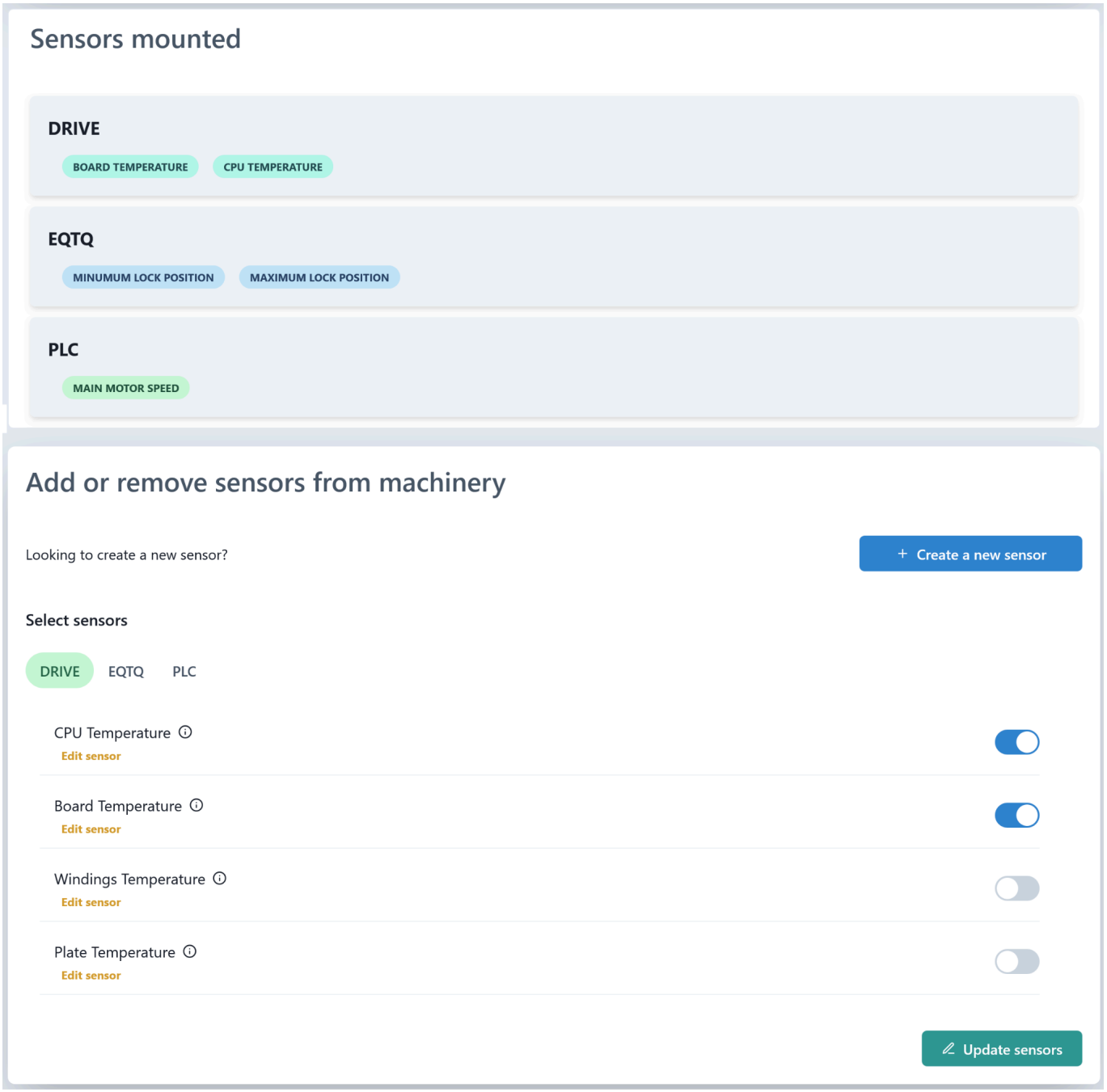


This feature has been incorporated into the extended version of the project with the primary objective of facilitating the deletion of machinery when necessary. The functionality incorporates a deliberate two-step confirmation process to mitigate the risk of accidental deletions, requiring the user to click twice on the delete action for confirmation.

The actual deletion process is performed through database triggers, providing a comprehensive and secure approach to the removal of machinery-related information. These triggers manage the elimination of permissions associated with the machinery. Access rights are promptly revoked, ensuring that the machinery is no longer linked to any user. Moreover, ownership of documents associated with the machinery is seamlessly transferred to another designated user, preventing data loss and maintaining accountability within the system.

By implementing these measures, the system upholds a robust and secure machinery deletion process. This approach not only safeguards data integrity but also ensures that users exercise caution when initiating deletions, contributing to a more reliable and accountable system operation.

6.1.4. Sensor management



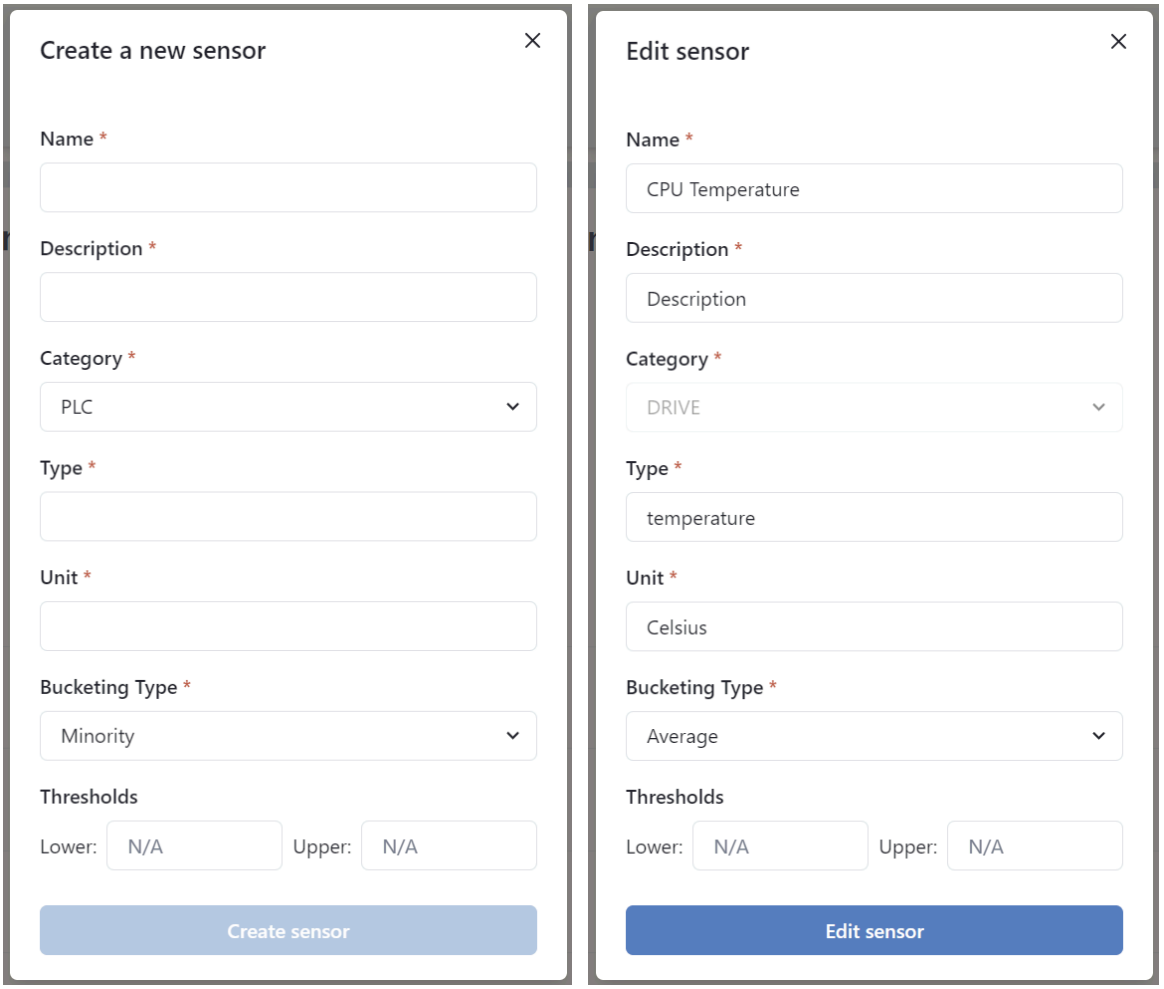
This module is designed to comprehensively manage the sensor catalog within the new web application. The concept of a sensor has been dualized in the database, leading to two distinct meanings that are handled separately. Firstly, the individual sensor is decoupled from any specific machinery, resulting in the creation of a general sensor catalog. This catalog comprises a comprehensive list of sensors, each with theoretical specifications, allowing for independent management without direct ties to any machinery. This flexibility enables the installation of the same sensor across different machines.

Secondly, for each machinery, there is a list of installed sensors, displayed prominently at the top of each machinery profile. The full catalog of sensors, categorized for ease of navigation, is accessible for each machinery. Users have the capability to choose which sensors should be installed or uninstalled by utilizing a toggle switch associated with each sensor. It's important to note that the deletion of a sensor is

treated as the uninstallation of the sensor from a specific machinery, and not from the general sensor catalog. This approach allows for the potential reinstallation of a sensor in a new machinery.
Access to this entire feature is granted to every AROL user, but specific restrictions are applied based on user roles:

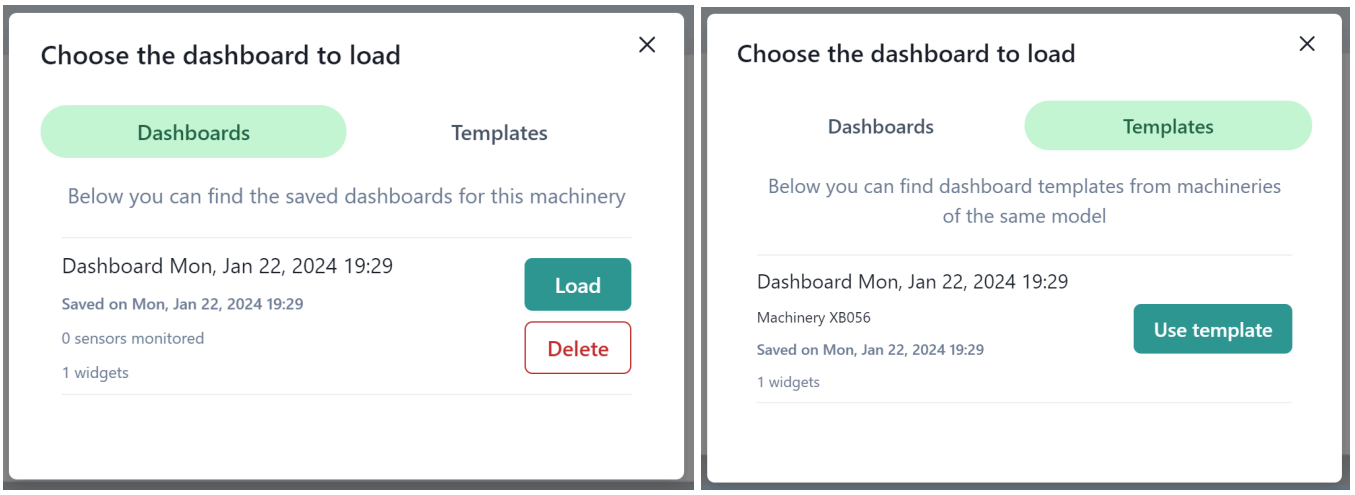
- Chief users have full permissions on sensors, allowing them to modify, install, and uninstall sensors without any restrictions.
- Supervisors can modify the set of installed sensors, but this permission is contingent upon having the necessary permissions on the associated machinery.
- Officers have a more limited scope and can only view the list of installed sensors on machinery. Their permissions do not extend to modifying or installing/uninstalling sensors.

This role-based access control ensures that users with different responsibilities within the AROL system have appropriate and restricted access to sensor management functionalities, contributing to a more secure and organized system operation.



The creation and update of sensors are facilitated by the same module, as depicted in the provided images. During the creation of sensors, users are required to define mandatory fields that are essential for accurately characterizing the sensor. Notably, sensors are categorized, and this categorization is integral to determining specific technical aspects associated with the sensor. Consequently, the category of a sensor plays a crucial role in defining its technical attributes, and as such, it cannot be changed once assigned.

6.2. Machinery dashboard templates support



The creation of a template is implicitly triggered each time a machinery dashboard is created within the system. A template, in this context, refers to a predefined dashboard structure that is strategically designed to simplify the management and monitoring of dashboards, particularly for users who may not possess technical expertise.

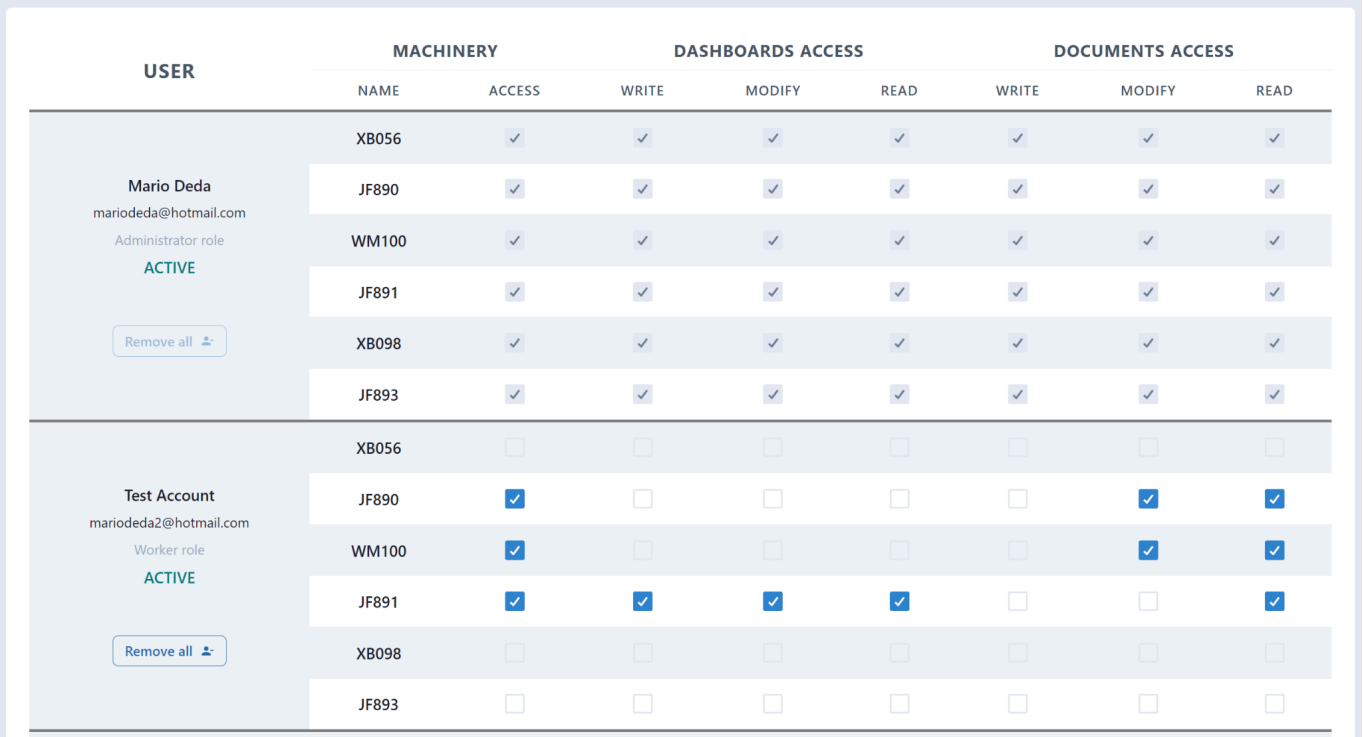
When a dashboard is created, the system automatically generates a template for each machinery that shares the same model as the machinery under consideration. This approach is rooted in the technical similarities shared by machineries of the same model. Additionally, a template is also created for the specific machinery being considered, to ensure a reuse approach for dashboard management.

The update of a template is intrinsically linked to a dashboard; specifically, whenever changes are saved to a dashboard, the associated template undergoes an update as well. This dynamic relationship ensures that the template accurately reflects the most recent configurations and content of its associated dashboard. Importantly, the system does not retain a reference to the old template, emphasizing a streamlined approach that focuses solely on updated dashboards and their corresponding templates.

By maintaining this one-to-one connection between dashboards and templates and discarding references to older templates, the system ensures simplicity and efficiency in managing updates. This design choice prioritizes the latest dashboard configurations, eliminating the need to manage multiple template versions for the same dashboard.

Given the established binding between a dashboard and its associated template, the deletion of the template is inherently tied to the removal of the corresponding dashboard. In other words, when a dashboard is deleted, the system ensures that its linked template is also automatically removed.

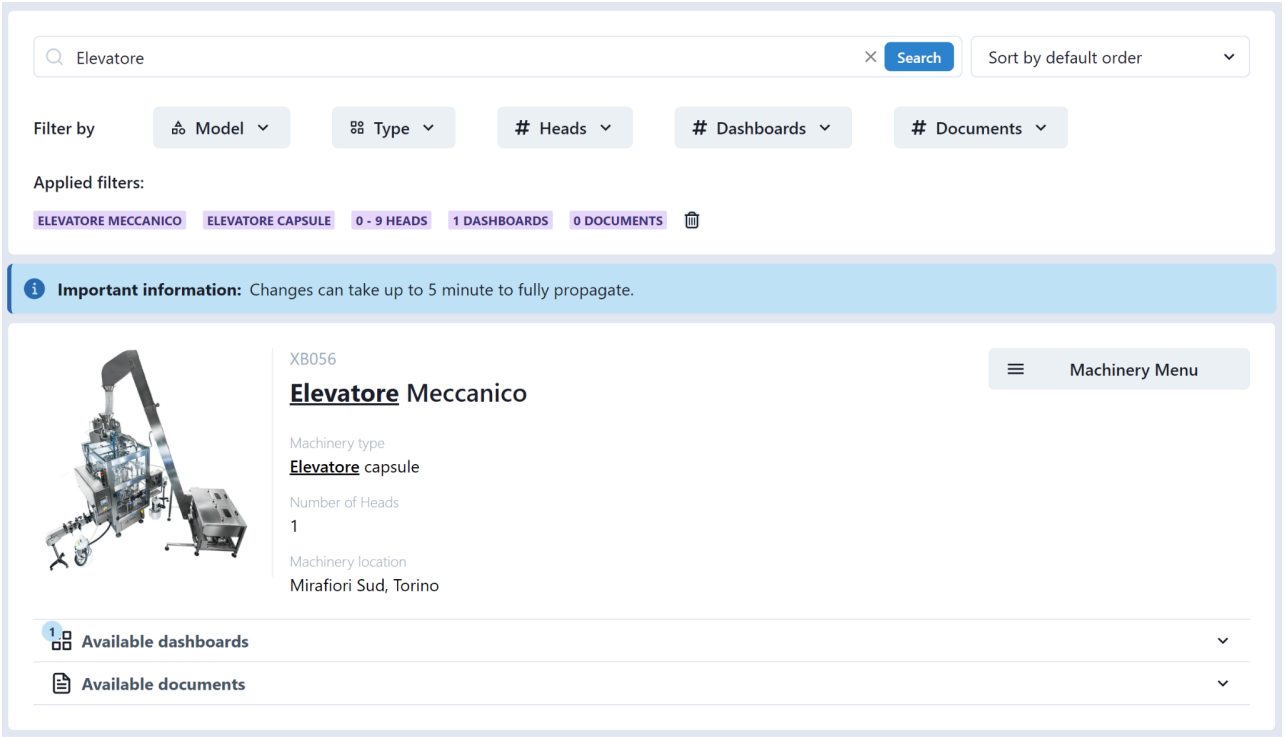
6.3. Management of machinery access permissions



USER	MACHINERY		DASHBOARDS ACCESS			DOCUMENTS ACCESS		
	NAME	ACCESS	WRITE	MODIFY	READ	WRITE	MODIFY	READ
Mario Deda mariodeda@hotmail.com Administrator role ACTIVE Remove all	XB056	✓	✓	✓	✓	✓	✓	✓
	JF890	✓	✓	✓	✓	✓	✓	✓
	WM100	✓	✓	✓	✓	✓	✓	✓
	JF891	✓	✓	✓	✓	✓	✓	✓
	XB098	✓	✓	✓	✓	✓	✓	✓
	JF893	✓	✓	✓	✓	✓	✓	✓
Test Account mariodeda2@hotmail.com Worker role ACTIVE Remove all	XB056	☐	☐	☐	☐	☐	☐	☐
	JF890	☑	☐	☐	☐	☐	☑	☑
	WM100	☑	☐	☐	☐	☐	☑	☑
	JF891	☑	☑	☑	☑	☐	☐	☑
	XB098	☐	☐	☐	☐	☐	☐	☐
	JF893	☐	☐	☐	☐	☐	☐	☐

In terms of the user interface, the base user permission grid has been retained graphically but has undergone updates. New controls have been incorporated to validate whether a user can grant granular permissions on specific machinery aspects. This graphical refinement aims to enhance the user experience and maintain consistency within user roles, ensuring a clear and intuitive representation of the permission system.

6.4. Machinery filtering and search



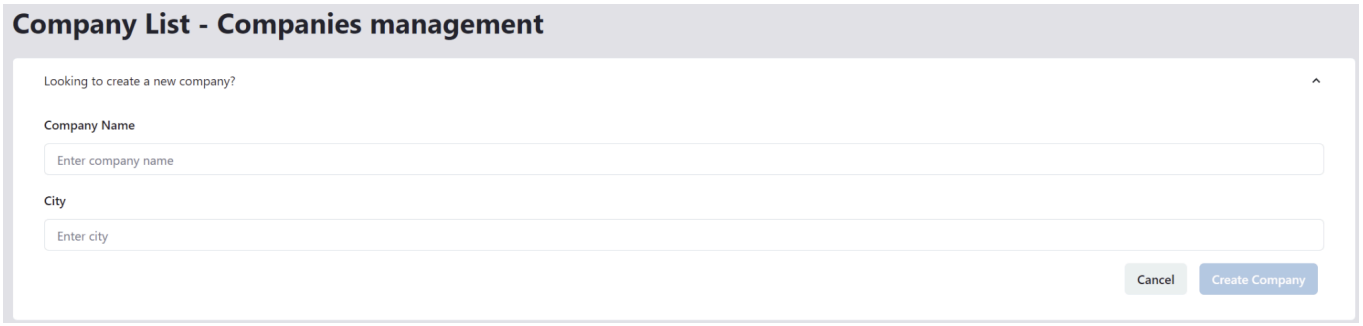
The filter and search component for machineries operates in a manner analogous to the user filter. The search term is intersected with applied filters to refine and customize search results. The designed filters for machineries are the following:

1. **Model and Type:** These filters allow the specification of single or multiple values for machinery models and types. They serve as checks to ensure that machineries meet specified criteria regarding both model and type.
2. **Number of Heads, Dashboards, and Documents:** These filters represent numerical ranges, with the minimum typically set at 0 or 1 for heads, and the maximum corresponding to the highest possible value for each filter across all machines. For dashboards and documents, certain restrictions are applied. In the context of company users, where dashboards and documents pages may be separated based on permissions, the associated filters are also separated. Consequently, some users might not see both options depending on the permissions granted. In contrast, for AROL users, permissions are not as fine-grained but are total. Thus, an AROL user could either see both or none of them, contingent on their permissions.

---

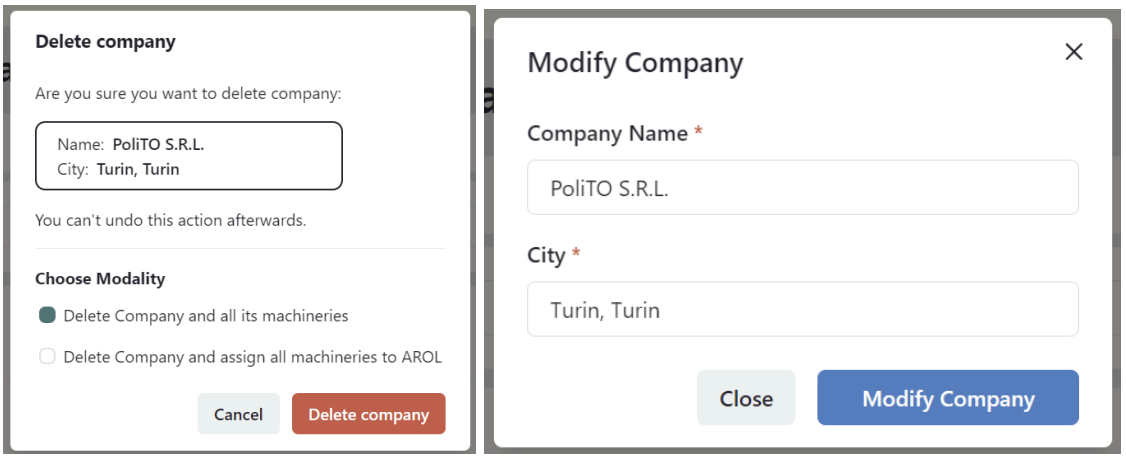
7. Additional Features

7.1. Module for creation and management of a new company

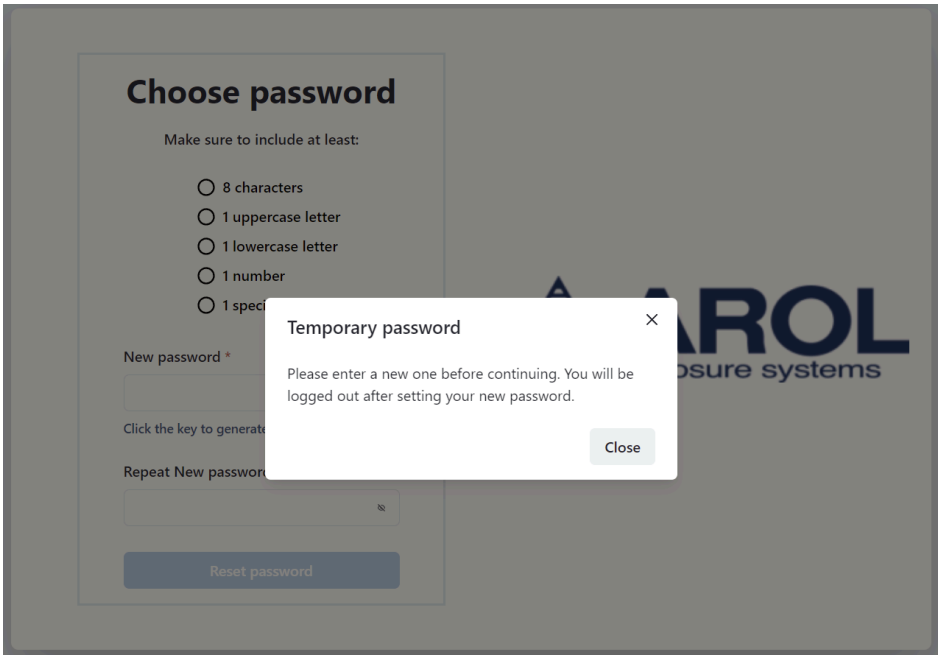


Company management modules have been developed to simplify AROL user operations. These modules enhance the management flow for both machinery and users, as they encompass both AROL and company entities within the concept of a company. Each company is uniquely identified by an ID, where, as previously mentioned, it is set to 0 for AROL. Additionally, a company is characterized by a name and a site represented by a city. Users with Chief and Supervisor roles are granted the authority to create a new company in the system, allowing them to input the necessary information during the company creation process. Any modifications to company details are also handled accordingly..

The deletion of a company comes with certain constraints. The user seeking to delete a company must specify whether to delete its associated machinery or reassign them to AROL for potential reuse. This provision adds flexibility to the management of company machinery.



7.2. Management for a temporary user



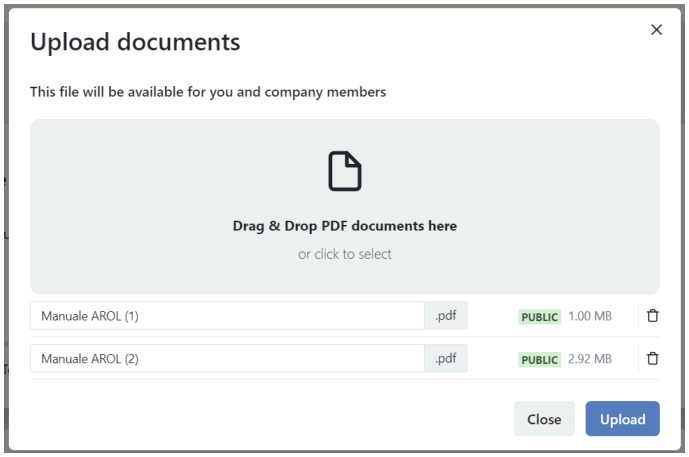
To address the privacy concerns associated with user passwords, an additional feature has been implemented. When an administrative user creates a new user for registration, they are now required to assign a temporary password. However, to ensure user privacy, the system introduces a temporary state for the user. This means that upon the user's initial login, they must choose their own password, preventing the administrative user from having knowledge of the user's login credentials.

In the event that a user needs to reset their password, the system automatically logs them out. Subsequently, the user can immediately access the system using the newly created credentials. This design ensures that the user's status within the system remains consistent with the database.

To facilitate this mechanism, a temporary status flag has been introduced into the user schema within the database, keeping the implementation straightforward and effective in managing user access and password privacy.

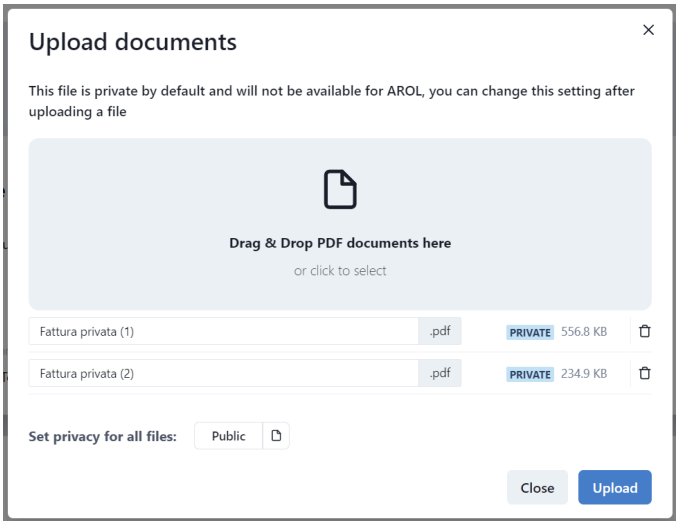
7.3. File privacy strategy

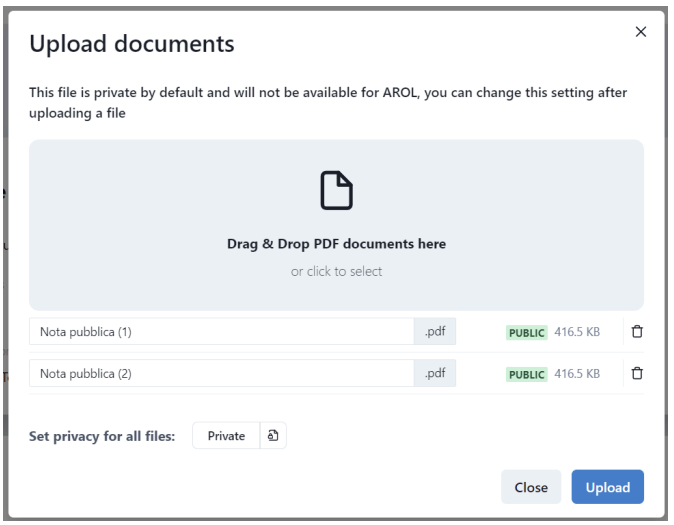
This feature has been implemented to enhance file privacy, particularly concerning machinery documents. Depending on the user's affiliated company, documents can now be uploaded as either public or private. The following breakdown outlines the various scenarios:



The AROL user is now limited to uploading only documents marked as public. This restriction is in place to facilitate the sharing of essential information between the supplier (AROL) and the customer company. Examples of such documents include technical sheets, user manuals, warranties, and more. These materials are considered cases of publicly viewable documents within the supplier and customer relationship.

This restriction ensures that the AROL user can only upload documents that are intended for broader visibility and collaboration, aligning with the need for transparency and information sharing between the supplier and the customer company. The focus is on facilitating effective communication and support by providing access to relevant documentation while maintaining the necessary level of privacy for other types of sensitive information.

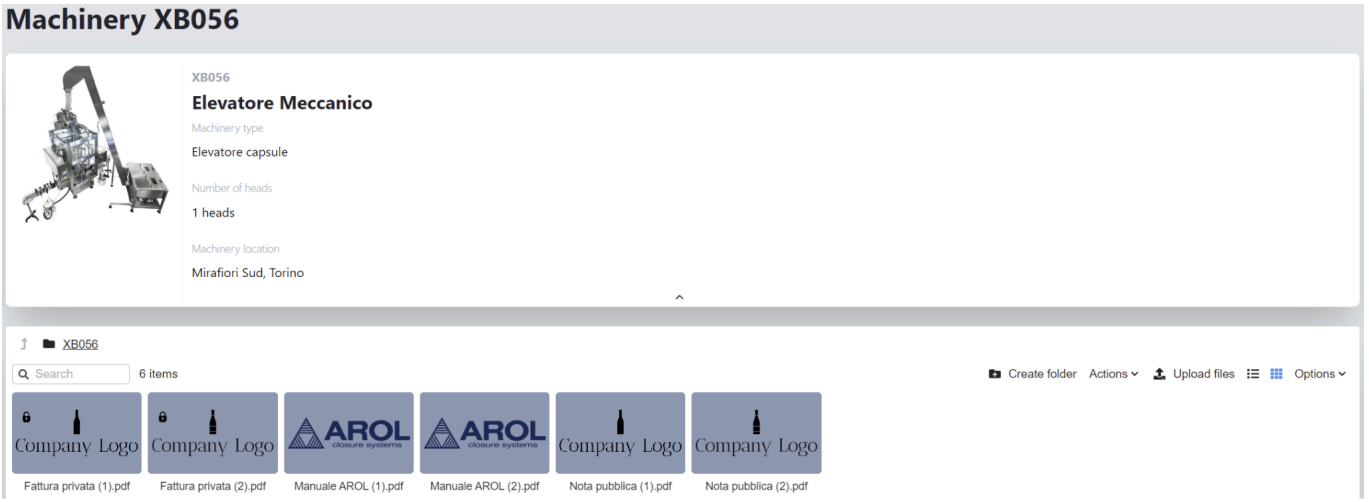




For company users, the document upload functionality has been extended to allow the upload of both private and public documents associated with a machinery. This expanded capability provides customer company users with increased freedom, flexibility, and privacy when managing machinery documents.

Private Documents: Users within a company can upload private documents, ensuring that these documents are accessible only within the company context. These may include sensitive internal reports, proprietary information, or documents intended solely for internal use.

Public Documents: Additionally, users have the option to upload public documents that are visible to AROL. This facilitates collaboration and communication between the customer company and AROL, allowing for the sharing of reports, technical issues, and assistance requests.



By offering this dual functionality, the system allows for a versatile approach to document management. Users can decide how to upload their documents based on the nature of the content, choosing between private documents for internal use and public documents for collaborative purposes with AROL. This ensures that users have the freedom to maintain privacy when needed, while also enabling effective cooperation and information sharing where applicable.

7.4. File ownership update on owner deletion

This feature has been designed and implemented with the primary objective of maintaining a consistent association between files and existing users. In the event that a user is deleted, any files linked to them will not be left orphaned. Instead, the user ID associated with these files will be replaced by the ID of the highest-ranking user within the same company. This ensures that all files remain under the management of an active user. However, if there are no remaining users within that company, the system will raise an error. This is to prevent files from being left without a responsible user.