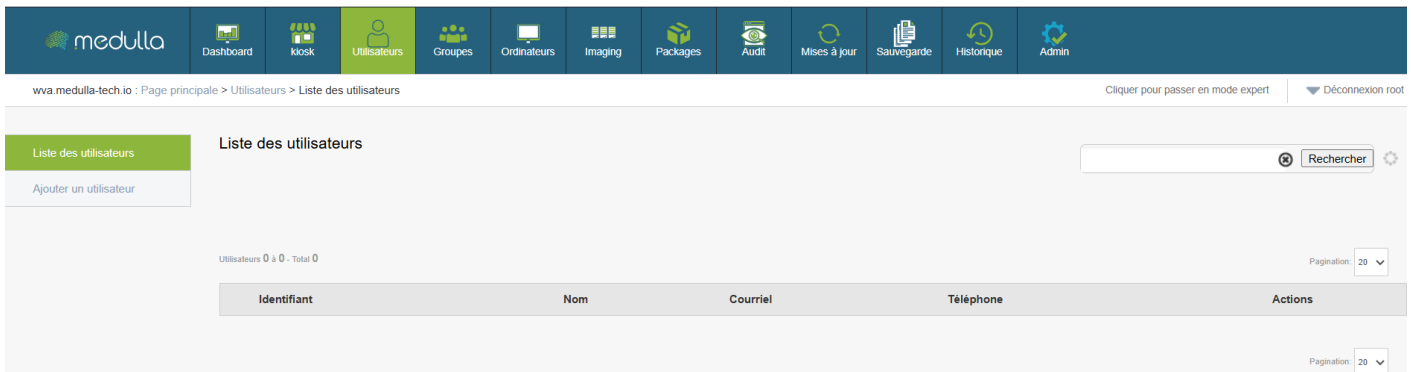


Chapter 4: Users

- [User Management in Medulla](#)
- [Add User](#)

User Management in Medulla





This section guides you in user management within Medulla. You will learn how to consult existing users, add new ones, assign them roles and organize them into groups.

Unlike the module *Kiosk*, which focuses on direct interaction, here the aim is to structure access and enhance security through clear permissions.

The User List section

Located in the centre of the screen, this section displays all registered users in your Medulla environment.

Identifiant	Nom	Courriel	Téléphone	Actions
 01202154	Jean DUPONT			   

Existing users

If users have already been created, they will appear as a table with the following information:

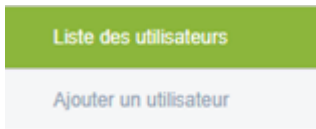
- **Identifiant** : the unique number assigned to the user.
- **Name** : full user name.
- **Email** : registered email address.
- **Phone** : telephone number (if indicated).
- **Actions** : options for **modify** or **delete** user.

No registered user

If no user has been added again, the central section will remain empty. A message will show that no user has been saved.

[See how to add a user](#)

Add User



To create a new user in Medulla, everything happens in the left side column.

A screenshot of the 'Ajout d'un utilisateur' (Add user) form in the Medulla application. The form is located in the left sidebar and contains the following fields: 'Identifiant*' (required), 'Mot de passe*' (required), 'Confirmation du mot de passe*' (required), 'Photo' (with a placeholder image and a button to 'Choisir un fichier'), 'Nom de famille*' (required), 'Prénom*' (required), and 'Titre'. The form is titled 'Ajout d'un utilisateur' and 'Attributs utilisateur'.

Accessing Creation

Click the link **Add User** to open the creation page.
The form will be displayed in the centre of the screen.

Complete the Creation Form

Here are the fields

- **Identifiant** : a unique identifier for this new user.
- **Password** and **confirmation** The password that will allow the user to log in.
- **Photo** (*optional*) : possibility to upload a profile photo.
- **Surname / First name**
- **Email**
- **Phone** and **Mobile**

User groups

Groupe primaire: MedullaUsers

Tous les groupes

GroupeTest1
MedullaUsers

Groupe(s) de l'utilisateur

Groupe(s) secondaires

Droit d'entité: Public, Statique, Super-Admin, Recursive

Supprimer

Add entity right

Valider Annuler

Group organisation makes it easy to manage access rights.

- **Primary group** : the main group to which the user belongs.
- **Secondary groups** : other groups to which you can add to extend its rights.

Define access rights (Entity rights)

At the bottom of the form you can set user access rights through several options:

- **Public**
- **Super administrator**
- **Recursive**
- **Statistics**




These options define the scope of actions that the user can perform in Medulla.

Finalizing the creation

Once all the fields are completed, click on .

The user will then be automatically added to the **List of Users**, visible in the centre of the main page

Edit an existing user

Identifiant	Nom	Courriel	Téléphone	Actions
 01202154	Jean DUPONT			   

At any time, you can change the information of an existing user.

- Go to the **List of Users** (centre of page).
- Locate the user concerned.

- Click **Modify** in the column "Actions"
- Update the required fields (name, email, groups, roles, etc.).
- Save the changes.

Modify MMC Rights

To adjust a user's access rights in Medulla, you can change its **MMC rights (also called ACLs - Access Control Lists)**.

Quick access to MMC rights

since **List of users**, click on the small **Key**  located to the right of the user line.

You will be redirected to the page .

You will see **complete list of modules and pages** de Medulla, sorted by categories Users, Groups, Computers, Logs, Imaging, etc.

- **Medulla's global logs**, grouped by Kiosk module, Imaging, Remote Desktop, Backup, etc.
- **Past actions by all users** according to its level of access
- **The date, user, and nature of each action** Profile creation, group modification, machine removal
- **Technical details** related to each action (IP, targeted machine, state, etc.)

If no **not rights** on a module (e.g. **not see logs** associated with this module in history, even if access to history is allowed.