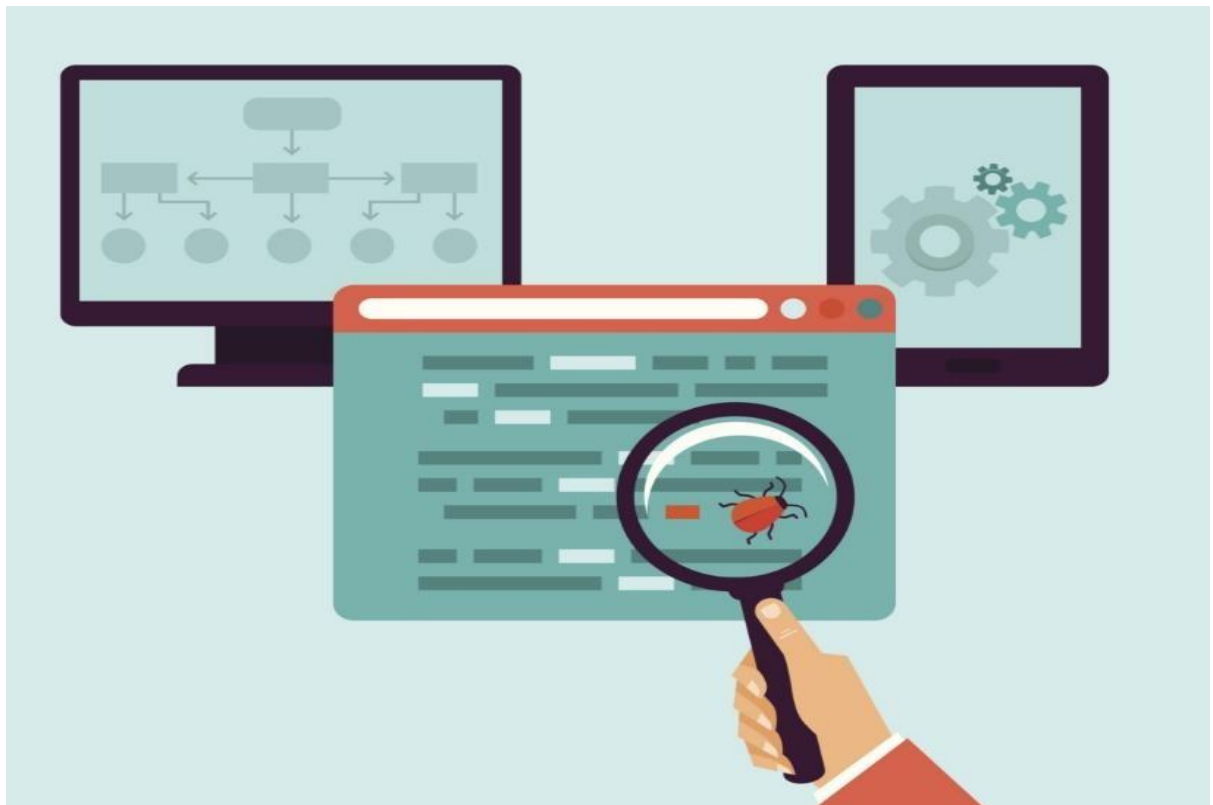Maintx Maintenance Management System

Employees
## Security And Setting
Access Rights

Security

After creating a new employee (see "**Employees**, adding new employees & assigning access"), we set the **security & access rights**.

The system security menu deals with setting the access rights for the users. The access rights differ from person to person, where all the users cannot be given the same permission.

The **access right** is only set by the **administrator** or the **supervisor** and not by any person below this level.
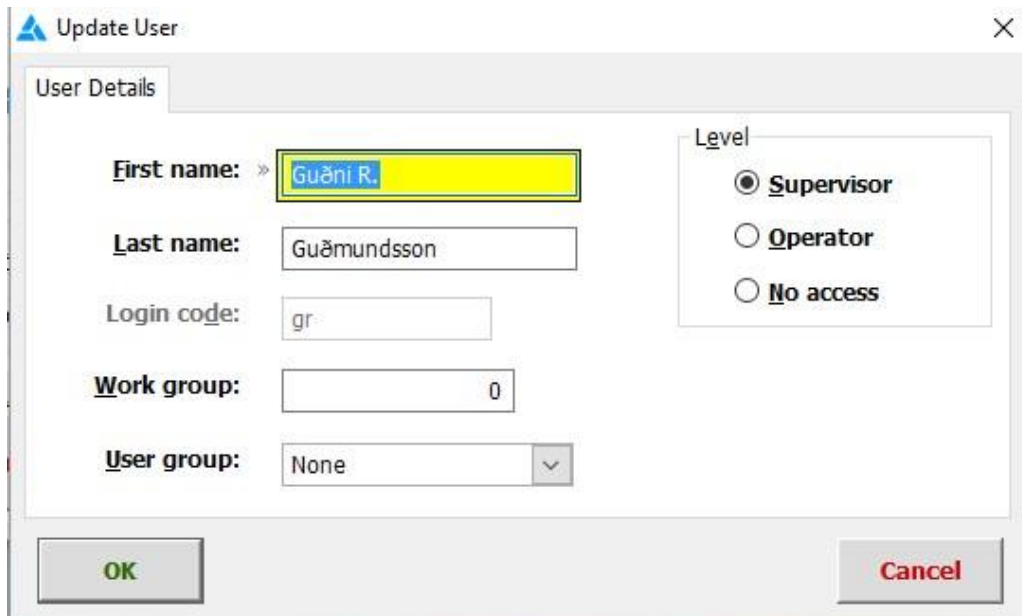
Let´s have a look at how the administrator sets the access rights for the new users. We start by going to "**File**" and pressing "**Security**".
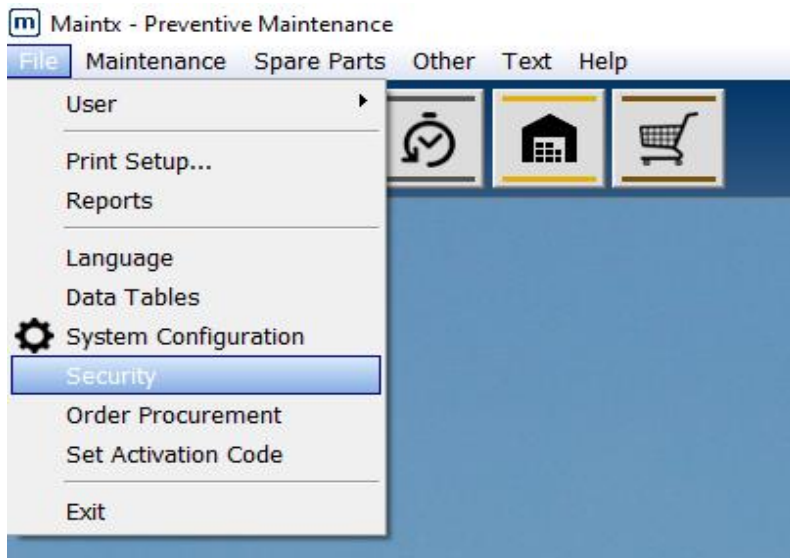
We get the "Browse users" menu.

maintx
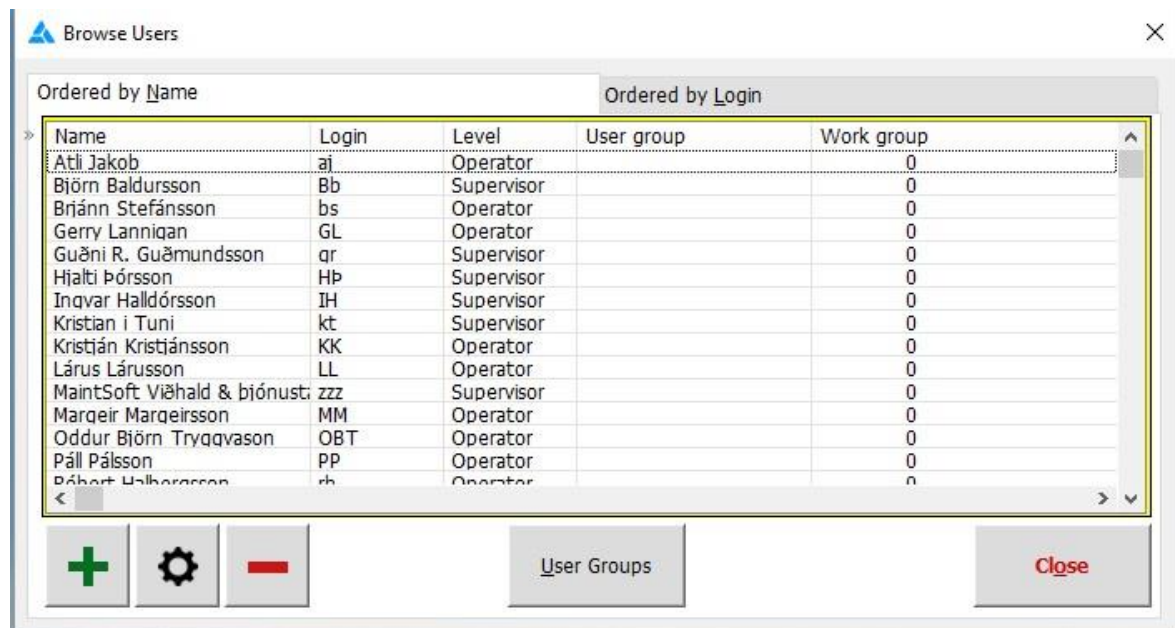
This window allows the administrator to determine the operational Level of the User. Start by selecting an already registered user and click the ⚙ button. Or double-click the name.

There are three different levels of operation available:

➢ Supervisor = Allowed to execute any and all operations in Maintx.

➢ Operator = Can only access those things the Supervisor allows them to.

➢ No access = Revokes any and all access to the chosen User.

We **don´t** need to define permission for the **Supervisor** since he has an all access pass.

The **Operators** permission is defined by the **Supervisor/Administrator**.

For every screen in Maintx you can press **CTRL** & **F8** and get a list of all users and the columns they are allowed to see on that screen.

For instance here we go to "**Workbook**"

Press **CTRL** & **F8**

In this case we don't want the user Haukur Gunnarsson to be able to see the "**Total Cost**" of the tasks.

We find the row with Haukur Gunnarsson and the column with the total cost, double-click the "yes" to change it into a "No" …   And press   OK
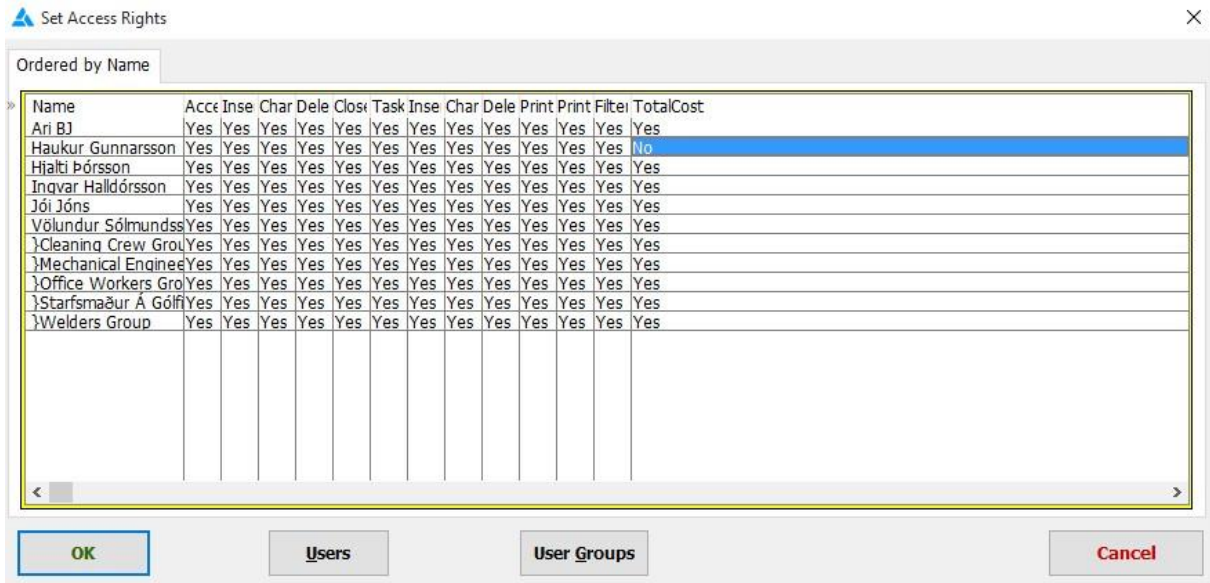
Next time Haukur Gunnarsson logs into Maintx, the **column** stating the **total cost will not be visible** to him.
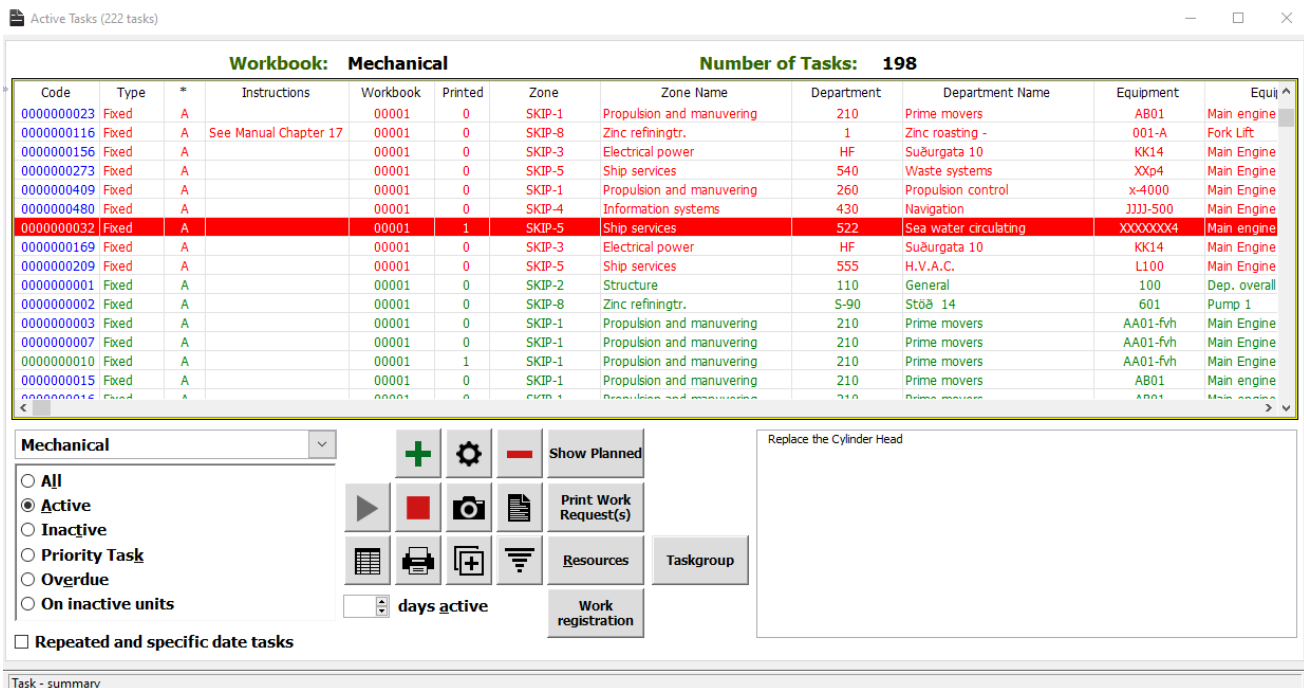
The same goes for most other columns, buttons and actions in Maintx. We can decide if a user can **Insert, Change, Delete, Print, Filter or close tasks**, to name just a few.

This can also be used to restrict access to certain areas or allow access to only one or two department or even just one or two equipment.

No access mode is kind of self-explanatory =>   User is **not allowed** any access rights at all.