



Content

1	Introduction on the new user right As from November 2023 in Easy to Inspect.....	2
2	Roles.....	6
2.1	Change a role	6
2.2	Assign a role to a user	8
2.2.1	Assign via the Role menu.....	8
2.2.2.	Assign via the My user menu	9
2.2.3	New Users	11
3	Groups	12
3.1	Introduction to Groups	12
3.2	Create a Group.....	12

1 Introduction on the new user right As from November 2023 in Easy to Inspect

Were previously, Easy to Inspect allowed 13 user rights per user, we have completely changed this set up as per Q4 2023. This enables (larger) organisations to be more flexible and design the use of Easy to Inspect specifically to their needs.

Before we explain how you can define the user rights within Easy to Inspect, we will explain terms we use within our tool. You need this basic understanding of our default settings, before you start changing or adding roles and groups.

User rights

Within Easy to Inspect a user can have different user rights:

C: Create: for instance, create an inspection, an action, an analysis

R: Read: for instance, read an inspection report

U: Update: for instance, change an inspection report, complete an action report, change an analysis

D: Delete: for instance, delete an inspection report.

Roles

These user rights are linked to roles within Easy to Inspect.

As a default we have defined 5 roles within Easy to Inspect. But specific organisations might create additional roles, to limit specific features of Easy to Inspect to their users.

Roles

System Admin: The user with this role can manage the account, the subscription and the users for the organisation.

Checklist Admin: The user with this role can make and manage the checklists (templates) for the organisation.

Inspect: The user with this role can do inspections (Mobile and Web) and access and manage their own inspections results.

Actions: The user with this role has access to the actions resulting from his/her own inspections and can manage these actions.

Analyse: The user with this role can use the analyse reports based on the data of all users.

The person who starts a trial account within Easy to Inspect will be assigned the 5 roles automatically. Every additional user within the account will be assigned the role Inspect.

Default features within the roles:

Role	User rights that can be selected at this role
System Admin	<ul style="list-style-type: none"> ✔ The user can manage the organisation. The user can manage and modify the subscription. The user can create, modify and delete users. The user can create and manage roles and user groups.
Checklist Admin	<ul style="list-style-type: none"> ✔ The user can create, modify and delete checklists for the organisation. The user can test unpublished checklists on the app. The user can create, change, and delete organization-specific filters. The user can create, change, and delete organization-specific reason codes. The user can manage automatic sending of inspection report based on filters. The user can manage automatic sending of action reports based on filters. The user can schedule automatic reminders for inspections.
Inspect	<ul style="list-style-type: none"> ✔ The user can perform inspections via the Mobile App and the Website. The user can create actions via the App (automatic background function with the OKNOK or score question, to be set per checklist). The user can send an email with an action report or inspection report (automatic background function, to be set per checklist). ✔ The user can read the own inspection data. ✔ The user can create reports of own inspections (including creating PDFs, exporting to Excel, and sending emails). ✔ The user can adjust own inspection results. ✔ The user can delete own inspection results and all the corresponding data.
Actions	<ul style="list-style-type: none"> ✔ The user can assign actions resulting from own inspections. ✔ The user can read actions resulting from own inspections (including creating PDFs, and exporting). ✔ The user can execute actions. The user can execute verifications. ✔ The user can delete actions resulting from own inspections.
Analyse	<ul style="list-style-type: none"> ✔ The user can create analyses with the inspection data of all users. ✔ The user can view and print these analyses. ✔ The user can adjust the analyses-settings. ✔ The user can delete these analyses.

Note: The tick box will link the rights to the role. The roles System admin and checklist admin / application link all rights to this role at once.

The System Admin can create new roles with specific features of Easy to Inspect.

Once the roles are established (the 5 default roles are defined as displayed above), users can be linked to the roles.

Groups and permission on groups

Organisations might be divided in multiple functional entities that operate apart from each other with Easy to Inspect. Because of geographical location, departmental activities etc.

A user with the role 'Inspect' can carry out an inspection, view and modify own inspection reports. The user with the role 'Action' can create action reports that result from own inspections, execute actions etc.

But these users of Easy to Inspect don't have access to the reports of other users. And they cannot read action reports of other users and assign actions of other users.

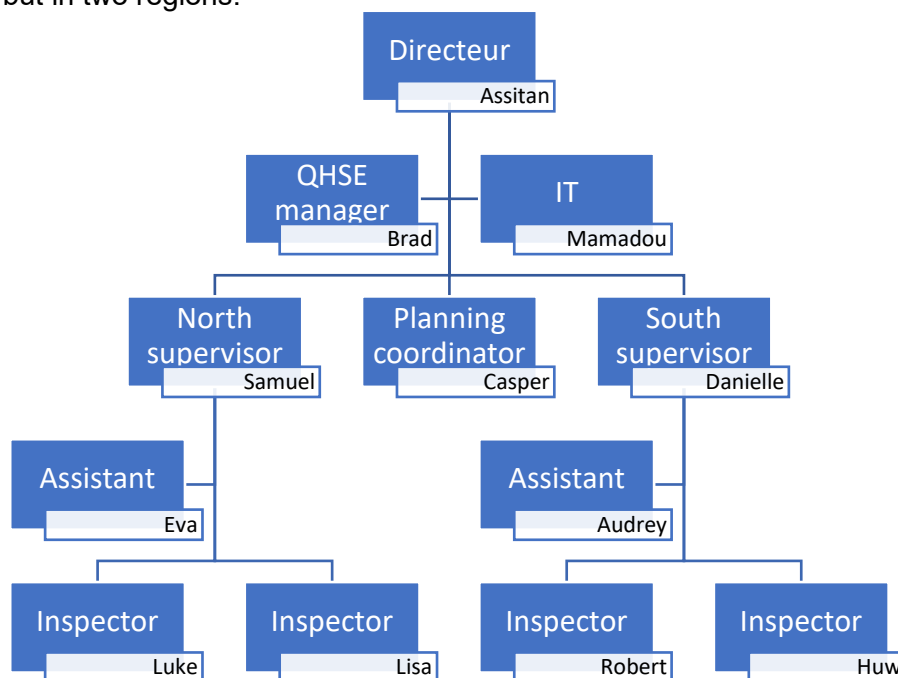
Several organisations would like department supervisors or coordinators, to have access to the inspection results and actions of employees within their team. It is possible to do so with the 'Group' function of Easy to Inspect.

It is possible to define groups of users and assign users to these groups that have permission on the inspection reports and nonconformity reports of other users that are part of this group. With such a set up, you can ensure that some users have access to all inspection reports, but other users can only access the reports of the group to which they were permitted. The users within the group themselves can only see their own inspection results.

Example

Let us explain this with an example:

In the following organisation chart a small company is presented working on the same activities but in two regions.



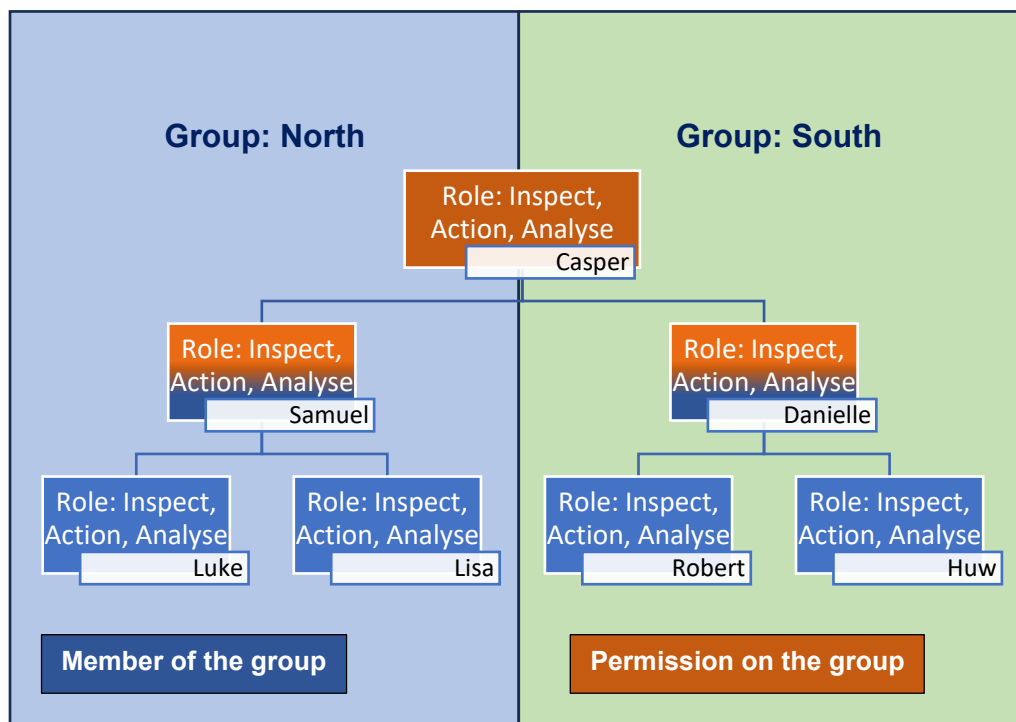
The basic role set up of Easy to Inspect is followed in this organisation:

- System admin
- Checklist admin
- Inspect
- Action
- Analyse

In all cases, each individual users with the roles Inspect & Action have the authority to create and modify their own inspections, assign actions on nonconformities of own inspections to other users. If you would like to allow certain users to view or even modify reports of other users, you must create a group and allow specific users, permission to view or modify these reports.

For instance:

1. Create a group North and South.
2. Define which users are entitled to manage results or actions of other users within the group. For instance, select Samuel as entitled user regarding the members of group North and select Danielle as entitled user regarding group South.
3. Define the permissions of the entitled user. What can the entitled users do with the reports of other users? For instance, modify inspection results (only possible if the checklist setting allows such), view or assign actions resulting out of inspections of other users etc.
4. Select the group members. These members are just grouped together. The users that are grouped together do not have the permission to view or manage the results or actions of other users in the group. That permission is only attributed to the entitled users (see step 2). In this example you would group the inspectors Luke and Lisa and supervisor Samuel to group North and inspectors Robert and Huw and supervisor Danielle to group South.
5. Furthermore, it would be convenient if the planning coordinator Casper can access the inspection reports of the members of both groups. So, grant Casper permission to the members of group North and South (step 2).

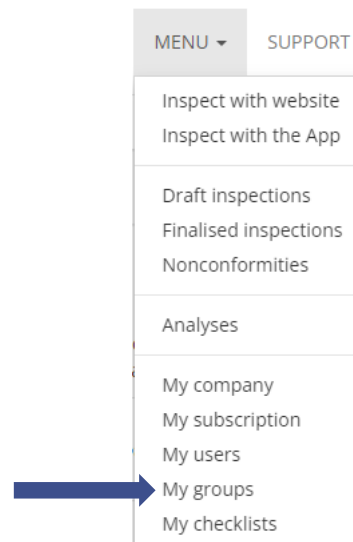


2 Roles

2.1 Change a role

Select the main menu: “My groups”

Note: If your menu does not show this option, you are not the account administrator or another user who has been assigned this role.



The “Roles”-menu will be displayed with the 5 default roles as defined in Easy to Inspect.

Dashboard / Roles & User Groups

Roles

A role is a group of permissions on system functions of Easy to Inspect. Roles are used to group permissions for easy user management. A user account can be assigned to one or more roles. Roles apply to the data of the user. [New role](#)


System Admin <i>The user with this role can manage the account, the subscription and the users for the organization</i>	Edit
Checklist Admin <i>The user with this role can make and manage the checklists (templates) for the organization</i>	Edit Delete
Inspect <i>The user with this role can do inspections (Mobile and Web) and access and manage their own inspections results</i>	Edit Delete
Actions <i>The user with this role has access to the actions resulting from his/her own inspections and can manage these actions</i>	Edit Delete
Analyse <i>The user with this role can use the analyse reports based on the data of all users</i>	Edit Delete

If you would like to edit the rights attributed to a Role select “edit”.

For instance, change the rights of the role Action by disabling the right that nonconformities that have been observed during an inspection can later be deleted.

Select “Edit” in the line ‘Actions’

Actions
The user with this role has access to the actions resulting from his/her own inspections and can manage these actions


Edit Delete

Select the tab “Permissions”

Dashboard / Roles & User Groups

Edit role: Actions

Role info Entitled users **Permissions**

A role grants access to system functions. A user can have one or more roles. Define a unique name for the role. You can add a description of the role.

Name of the role

Description of the Role

Save Cancel

and deselect the permission ‘The user can delete actions resulting from own inspections’.

Edit role: Actions

Role info Entitled users **Permissions**

Define what a user with this role may do in the system. A role grants access to system functions. Please choose the permissions that apply to this role.

System admin

- The user can manage the organization.
The user can manage and modify the subscription.
The user can create, modify and delete users.
The user can create and manage roles and user groups.

Application

- The user can create, modify and delete checklists for the organization.
The user can test unpublished checklists on the app.
The user can create, change, and delete organization-specific filters.
The user can create, change, and delete organization-specific reason codes.
The user can manage automatic sending of inspection report based on filters.
The user can manage automatic sending of action reports based on filters.
The user can schedule automatic reminders for inspections.

Inspections

- The user can perform inspections via the Mobile App and the Website.
The user can create actions via the App (automatic background function with the OKNOK or score question, to be set per checklist).
The user can send an email with an action report or inspection report (automatic background function, to be set per checklist).
- The user can read the own inspection data.
The user can create reports of own inspections (including creating PDFs, exporting to Excel, and sending emails).
- The user can adjust own inspection results.
- The user can delete own inspection results and all the corresponding data.

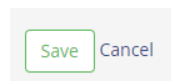
Actions

- The user can assign actions resulting from own inspections.
- The user can read actions resulting from own inspections (including creating PDFs, and exporting).
- The user can execute actions.
The user can execute verifications.
- The user can delete actions resulting from own inspections.

Analyses

- The user can create analyses with the inspection data of all users.

Then save your setting:

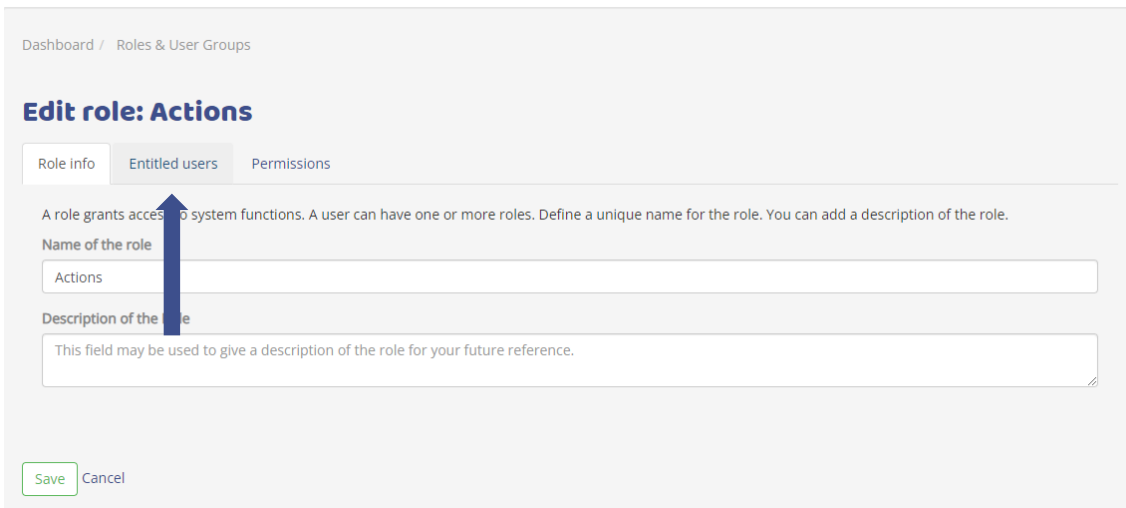


2.2 Assign a role to a user

If you would like to assign a role to a user, this can be done in two ways.

2.2.1 Assign via the Role menu

When you are working on a role already, it is easy to assign the user that is entitled this role. Simply select the Tab “Entitled users” and select one or more users that you would assign the role.



Dashboard / Roles & User Groups

Edit role: Actions

Role info | **Entitled users** | Permissions

A role grants access to system functions. A user can have one or more roles. Define a unique name for the role. You can add a description of the role.

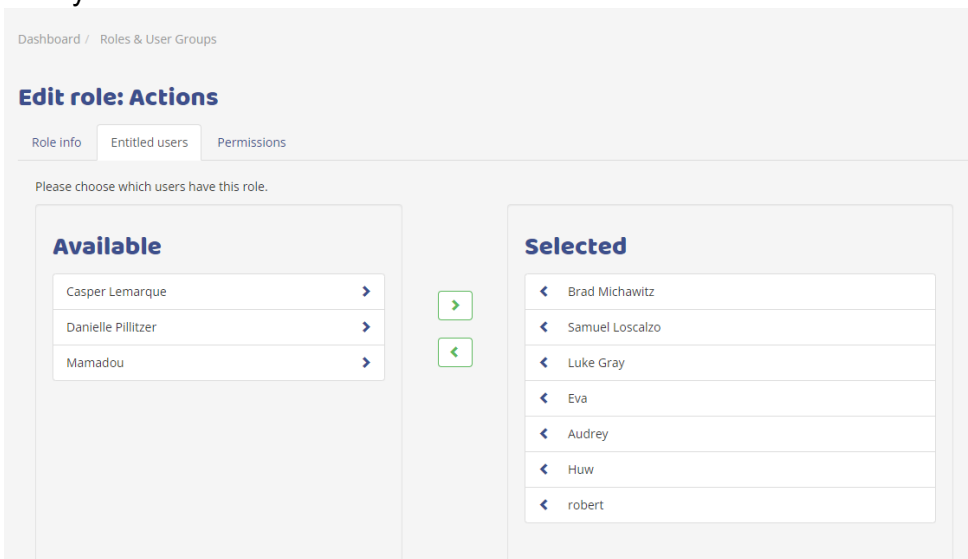
Name of the role

Description of the role

Save Cancel

A blue arrow points to the 'Entitled users' tab.

Now you can select or deselect users.



Dashboard / Roles & User Groups

Edit role: Actions

Role info | **Entitled users** | Permissions

Please choose which users have this role.

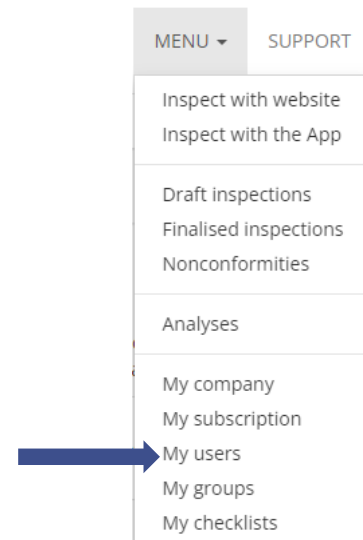
Available		Selected
Casper Lemarkue >	>	< Brad Michawitz
Danielle Pillitzer >	>	< Samuel Loscalzo
Mamadou >	>	< Luke Gray
	<	< Eva
	<	< Audrey
	<	< Huw
	<	< robert

Green arrow buttons are located between the Available and Selected columns.

Don't forget to save your setting.

2.2.2. Assign via the My user menu

Once a role is created, you can assign the role to a user. This can be done via the “My Groups” menu but also via the “My user” menu.



When you open the “My User” menu, the users in your account will be displayed. In the user overview, assigned roles and entitled groups are displayed per user. If you would like to set or change the roles (and or user groups), you select the ‘Action’ button.



manage / my users Help me

My users

[New](#)

You are using 9 of the maximum number of 10 users.

The user Audrey has been changed.

Name	E-mail	Your alternative E-mail address (receiver)	Roles and usergroups	Last updated (created)	
Audrey	audrey@easytoinspect.com	audrey@easytoinspect.com	Roles: Inspect, Actions, Analyse User groups: South	21-11-2023 (15-11-2023)	
Brad Michawitz	brad@easytoinspect.com	brad@easytoinspect.com test@easytoinspect.com	Roles: System Admin, Checklist Admin, Inspect, Actions, Analyse User groups: Admin all inspections, Admin all actions	21-11-2023 (28-02-2013)	

You can now change the settings of this user.

Click on the “Roles” to select one or more roles that you would like to assign to the user. More roles can be selected by combining the CTRL button and your mouse.

manage / my users / modify user Help me

Edit user ?

Name: Login E-mail: E-mail the results to: Language:

Additional text for report: Signature:

Password: Confirm password:

Roles and usergroups

Roles:

- System Admin
- Checklist Admin
- Inspect**
- Actions
- Analyse

User groups:

- Admin all inspections
- Admin all actions
- North

After you have made your selection, save your settings.

Roles and usergroups

Roles:

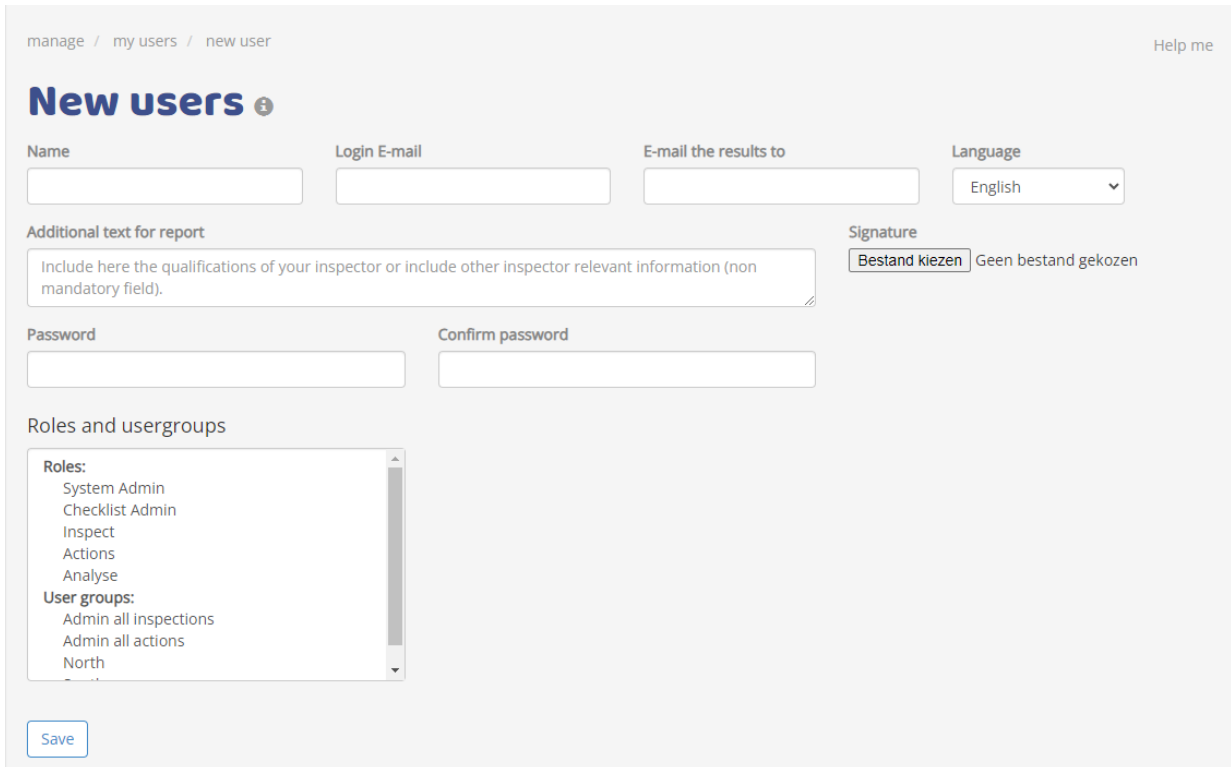
- System Admin
- Checklist Admin
- Inspect**
- Actions
- Analyse

User groups:

- Admin all inspections
- Admin all actions
- North

2.2.3 New Users

Via the “My User” menu you can select “new user”.
The new user can be assigned Roles. The roles contain user rights.



manage / my users / new user Help me

New users

Name

Login E-mail

E-mail the results to

Language

Additional text for report

Signature Geen bestand gekozen

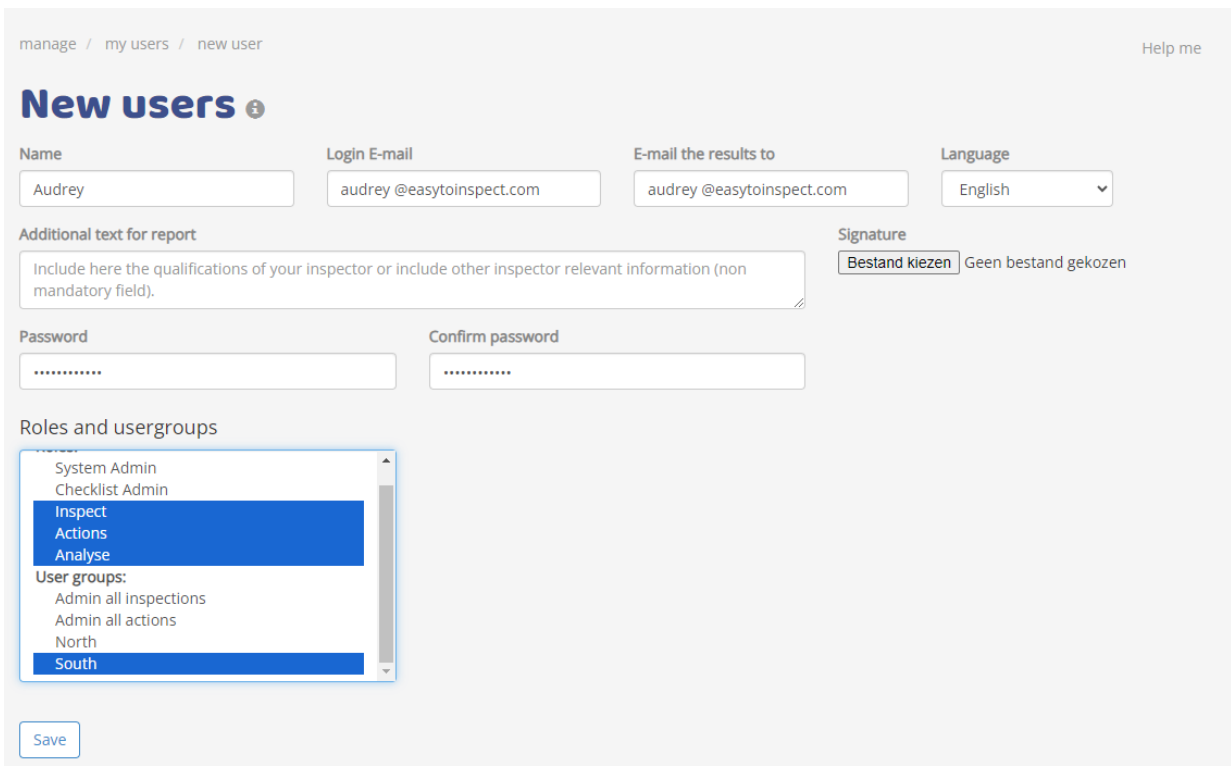
Password

Confirm password

Roles and usergroups

- Roles:
 - System Admin
 - Checklist Admin
 - Inspect
 - Actions
 - Analyse
- User groups:
 - Admin all inspections
 - Admin all actions
 - North
 - South

Click on the “Roles” to select one or more roles you would like to assign to the user. More roles can be selected by combining the CTRL button and the mouse.



manage / my users / new user Help me

New users

Name

Login E-mail

E-mail the results to

Language

Additional text for report

Signature Geen bestand gekozen

Password

Confirm password

Roles and usergroups

- Roles:
 - System Admin
 - Checklist Admin
 - Inspect
 - Actions
 - Analyse
- User groups:
 - Admin all inspections
 - Admin all actions
 - North
 - South

Save your settings when you are finished.

3 Groups

3.1 Introduction to Groups

Organisations might be divided in multiple functional entities that operate apart from each other with Easy to Inspect. Because of geographical location, departmental activities etc.

A user with the role Inspect can carry out an inspection, view own inspection reports. The user with the role Action can create action reports that result from own inspections, execute actions etc.

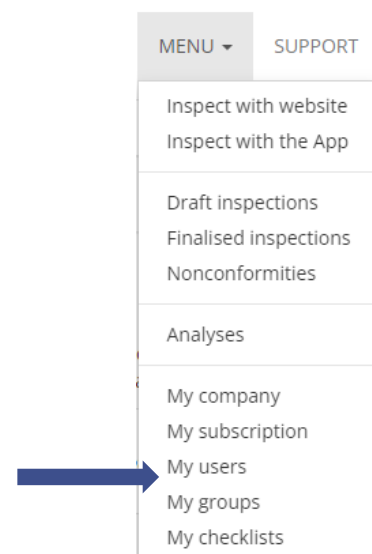
But these users of Easy to Inspect do not have access to the reports of other users, and they cannot read action reports of other users and assign actions of other users.

Several organisations would like department supervisors or coordinator, to have access and even control of the inspection results and actions of employees within their team. It is possible to do so with the 'Group' function of Easy to Inspect.

Within Easy to Inspect, 2 default user groups "All inspections" & "All Actions" are defined. The administrator is entitled to view all inspections and actions by default. You can add additional users, however always 1 Easy to Inspect user must be entitled access to other users inspection reports and actions.

3.2 Create a Group

Select "My groups" via the main menu.



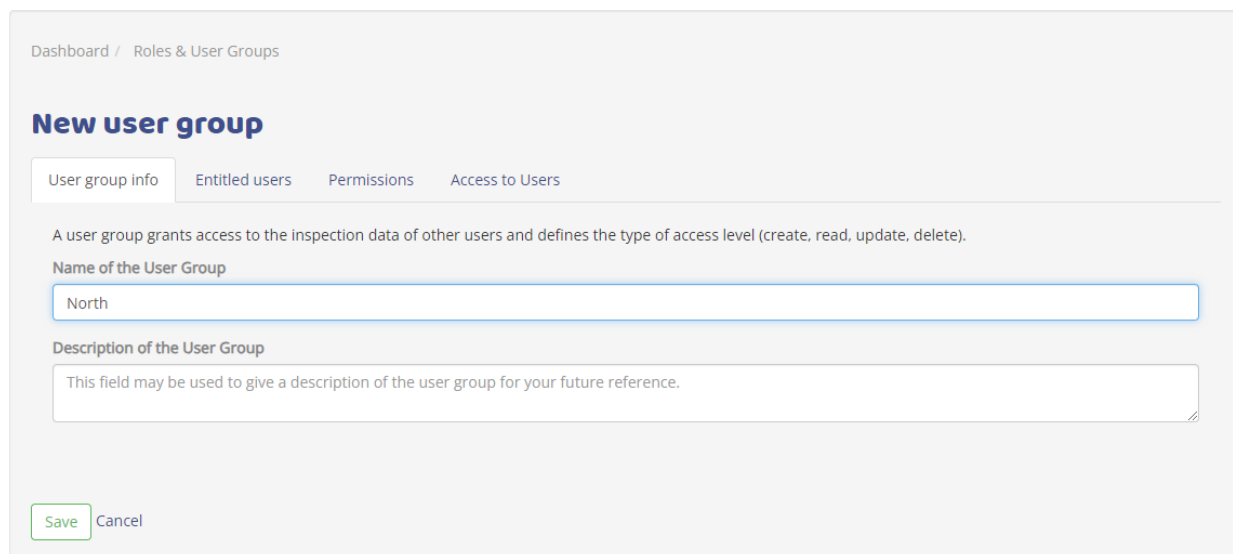
The Roles and User Groups screen will display.
Select new user group.



The new User group screen will be displayed. This screen is set up by means of 4 Tabs. Each Tab requires settings to create a user group.

Start with filling in your User Group's name. For instance, 'North'.

After filling in the name go directly to the second Tab, "entitled users". You only need to save when you have completed all 4 Tabs.



In the Tab "Entitled users", you select which users have permissions on the inspection results and action reports (nonconformities) of the other Easy to Inspect users that you will assign as group members (tab 4).

In this example; Samuel (the team leader of Team North) and Casper (planner) should have permission.

You can select the users by Clicking on the 'arrow' in the user box.

Dashboard / Roles & User Groups

New user group

User group info Entitled users Permissions Access to Users

The entitled users may use the inspection (and/or action) data from other users as defined in this user group. These users have access to the inspection data of other users. In the section "Access to Users" you define from which users the inspection data may be accessed/used.

Available

Brad Michawitz	>
Casper Lemarque	>
Luke Gray	>
Danielle Pillitzer	>
Mamadou	>
Eva	>
Audrey	>
Huw	>
robert	>

>

<

Selected

<

Save Cancel

If you would like to deselect, just click on the arrow in the column of selected users.

Available

Brad Michawitz	>
Casper Lemarque	>
Luke Gray	>

>

<

Selected

<

Once you have selected the "entitled users", you must define what permissions will be granted. Are these users entitled to read inspection results or are they also entitled to modify inspection results?

Attention: If a user of Easy to Inspect has no individual right of carrying out inspections (the role Inspect is not assigned to the user), this user cannot be granted permission regarding inspections of other users. The same applies to Action permissions.

If this might be the case, first assign the roles to the individual user (see 2.2.2), before you would grant group-permissions.

Select the permissions by clicking the tick boxes in the Tab “emissions”.

In the underneath example you see that Casper and Samuel have been granted permission to read, modify inspection results. They cannot delete an inspection result of other users.

Dashboard / Roles & User Groups

New user group

User group info Entitled users **Permissions** Access to Users

Define what the entitled users may do with the inspection data of other users that are assigned to the group. Choose which actions may be done with the inspection data of the other users.

Inspections

- The user can perform inspections for other users.
- The user can read inspections performed by other users.
The user can create reports of inspections performed by other users (including creating PDFs, exporting, and send emails).
- The user can adjust inspection results of inspections done by other users.
- The user can delete inspections (and all their corresponding data) done by other users.

Actions

- The user can assign actions resulting from inspections by other users.
- The user can read actions resulting from inspections by other users.
- The user can assign actions resulting from inspections by other users.
The user can execute assigned actions.
The user can perform verification of actions.
- The user can delete actions resulting from inspections by other users.

The last step is to assign users to the group. In this example, Group ‘North’ consists of following Easy to Inspect users.

Dashboard / Roles & User Groups

New user group

User group info Entitled users Permissions **Access to Users**

Define from which users the inspection data may be used. Select the users, that will be assigned to this user group. The inspection data of the users that are selected here can be accessed by the entitled users. E.g. all members of the Maintenance team or all employees of region South (organizational units). This group applies to all users, if no users are selected.

- All users
- Audrey
- Brad Michawitz
- Casper Lemarque
- Danielle Pillitzer
- Eva
- Huw
- Lisa
- Luke Gray
- Mamadou
- robert
- Samuel Loscalzo

When you are finished, save your settings.

You can always check your settings by clicking on editing your user groups.

User groups

A user group grants access to the inspection data of other users and defines the type of access level (create, read, update, delete). A user group defines what an entitled user is allowed to do with the data of other users (view, edit, delete, etc.). For example to view, edit, delete results of other members of your team.

New user group

Admin all inspections	Edit Delete
Admin all actions	Edit Delete
North	Edit Delete

If you would like to see, which user has permissions on what user group, you can also check via the “My user” menu. In our example Casper (and Samuel) are entitled to Group North which is displayed in the column “Roles and usergroups”.

manage / my users Help me

My users

You are using 10 of the maximum number of 10 users.

Name	E-mail	Your alternative E-mail address (receiver)	Roles and usergroups	Last updated (created)	
Audrey	audrey@easytoinspect.com	audrey@easytoinspect.com	Roles: Inspect, Actions, Analyse User groups:	21-11-2023 (15-11-2023)	Action
Brad Michawitz	brad@easytoinspect.com	brad@easytoinspect.com test@easytoinspect.com	Roles: System Admin, Checklist Admin, Inspect, Actions, Analyse User groups: Admin all inspections, Admin all actions	21-11-2023 (28-02-2013)	Action
Casper Lemarque	cl@easytoinspect.com	cl@easytoinspect.com	Roles: System Admin, Inspect User groups: North	15-11-2023 (28-02-2013)	Action