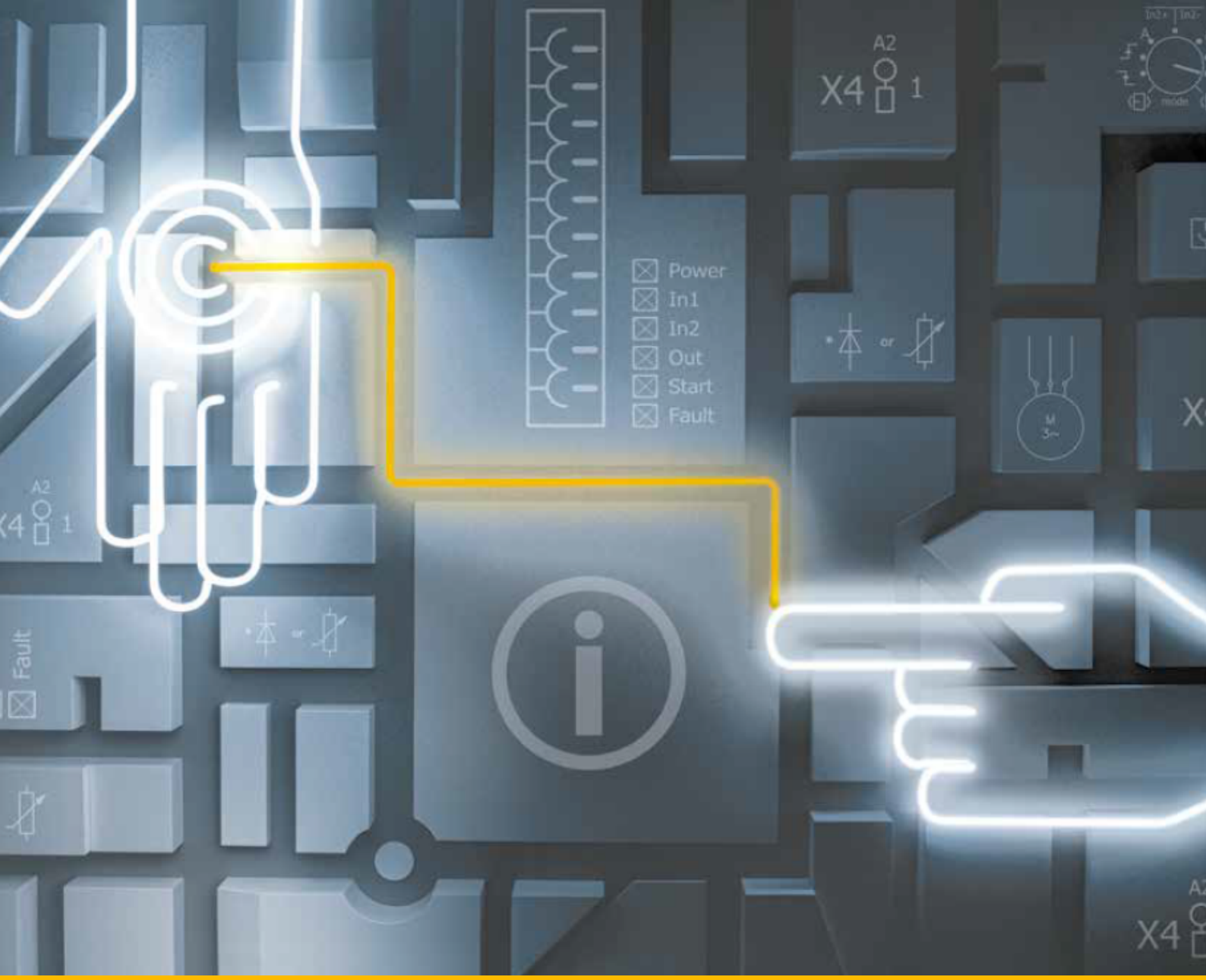


Myzel Lifecycle Platform

PILZ
THE SPIRIT OF SAFETY

Getting started-1006876-EN-02




This document is the original document.

Where unavoidable, for reasons of readability, the masculine form has been selected when formulating this document. We do assure you that all persons are regarded without discrimination and on an equal basis.

1 First steps on the Myzel Lifecycle Platform

In order to log into the Myzel Lifecycle Platform (MLP), your company needs a company account (tenant) for the Myzel Lifecycle Platform. Your company account is a closed area on the Myzel Lifecycle Platform, which exclusively contains your company's data.

When Pilz creates the company account, it also creates a user account within the company account for a named person from your company. This person is the MLP administrator for your company. The MLP administrator can create user accounts for additional persons and assign software roles to these persons.

The software roles assigned to a user determine the functions available to that user on the Myzel Lifecycle Platform.

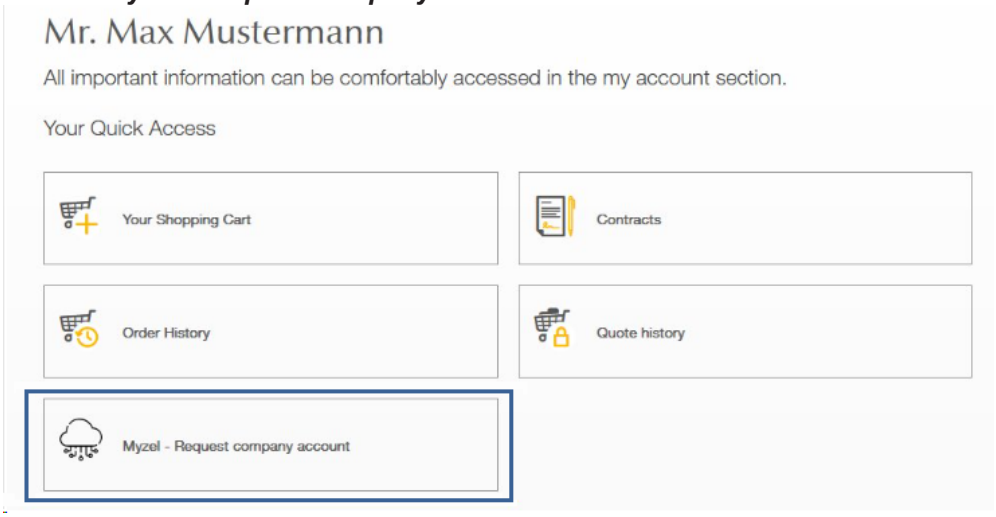
If you need a user account, please contact your MLP administrator.

1.1 Apply for a company account

Any employee of a company that is registered as a customer with Pilz can apply for a company account (tenant) for the Myzel Lifecycle Platform for their company. Each company can only have one company account.

Procedure

1. Log into the E-Shop
   ⇨ Open the Pilz E-Shop and log in.
2. Request company account
   ⇨ Click on ***Myzel - Request company account***.



Your company's request for a company account for the Myzel Lifecycle Platform will be processed. Once processing is complete, the selected administrator will receive an E-Mail to activate their user account.

Notes

- Delete company account
  If your company no longer wishes to use the company account, you can have it deleted. In the E-Shop, select ***Personal Details*** in your personal menu. You can apply for it to be deleted there.

1.2 Activate user account

If an account has been created for you, you will receive an E-Mail to activate the account. If you have not received an E-Mail, please also check the spam folder on your E-Mail account.

⇨ Open the E-Mail and click on ***Activate account***.

1.3 Open Myzel Lifecycle Platform

The Myzel Lifecycle Platform can be opened in an Internet browser. We recommend the Internet browsers Google Chrome, Mozilla Firefox and Microsoft Edge. Other Internet browsers can be used, but have not been tested.

⇨ Enter the URL https://cloud.pilz.com in your Internet browser.

1.4 Create new user account

Employees whose data is to be managed in the Myzel Lifecycle Platform (MLP) and employees who are to perform tasks in the MLP require an account.

There are two types of account:

- Main account
- Guest account

A company with a company account for the Myzel Lifecycle Platform can create user accounts for its employees. This is usually the employee's main account.
If a person is to have access to the company account, but already has a main account with another company, then a guest account can be created for them.
For example, an employee in Pilz's technical support has their main account for the MLP at Pilz. They can also have a guest account created for them with your company, to allow them to perform a machine validation for you, for example.

The type of account has no effect on access rights to the MLP. The actions a user may perform on the MLP are determined exclusively by the software roles assigned to them.

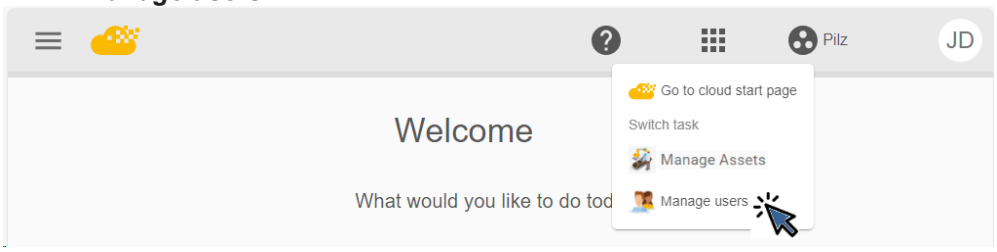
Prerequisite

- The action can be performed by users who have the following software role:
  - MLP administration
  - myAccessControl
  - Production management

Procedure

1. Open Myzel Lifecycle Platform [📖 5].
2. Open user management

⇨ Select ***Manage users*** in the menu:



3. Create user

   ⇨ Click on ***New user*** and enter the required data.
   Only activate the option ***User has MLP access*** if the employee is to perform tasks on the Myzel Lifecycle Platform.

   The user will now appear in the list of users.
   If you have activated the option ***User has MLP access***, the user will receive an E-Mail, to enable them to activate their account.

Notes

When you click on the ⋮ menu in the row of a user, you will find the following options in the list of users:

- Delete
  You can delete user accounts at any time.
- Disable account (only for users with MLP access)
  If a user is not to have access to their account temporarily, you can disable the account.
- Re-send activation E-Mail (only for users with MLP access)
  If a user has failed to activate their account within 3 days of receiving the activation E-Mail or they did not receive the activation E-Mail, you can re-send the E-Mail.

1.5 Assign software roles to users

The actions a user may perform on the Myzel Lifecycle Platform are determined by the software roles assigned to them.

Software roles on the MLP:

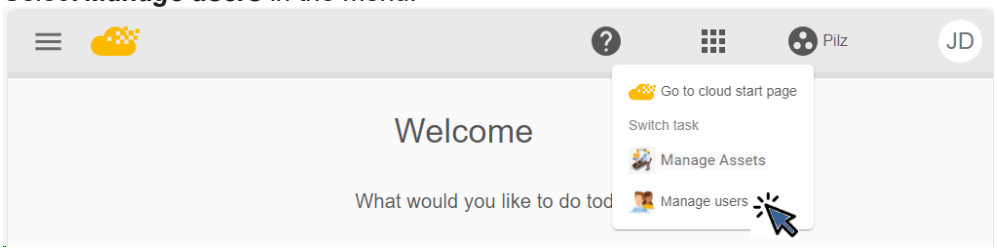
- MLP administration
  Role for a user who manages the user accounts in their company and provides technical support to those using the Myzel Lifecycle Platform (MLP).
  There must be at least one MLP administrator in each company. There may also be several. At least one of the MLP administrators must have their main account with the company. The other MLP administrators may have a main account or a guest account with the company.
- myAccessControl
  Role for a user who is responsible for managing safe and secure access to machinery. Tasks: asset protection, management of user permissions and identification keys. For this software role, it is necessary to purchase the corresponding subscription so that the tasks can be carried out.
- Production management
  Role for a user who is responsible for a company's entire production process. The production manager ensures efficiency, quality, compliance and productivity.
- mySafeDesign
  Role for a user who is responsible for the creation of safe machinery. Tasks: machine risk assessment, design validation. For this software role, it is necessary to purchase the corresponding subscription so that the tasks can be carried out.
- mySafeOperation
  Role for a user who is responsible for the (safe) operation of machinery. Task: operational validation (inspection). For this software role, it is necessary to purchase the corresponding subscription so that the task can be carried out.

Prerequisite

- The action can be performed by users who have the following software role:
  – MLP administration
- The user to whom software roles are to be assigned must have MLP access.

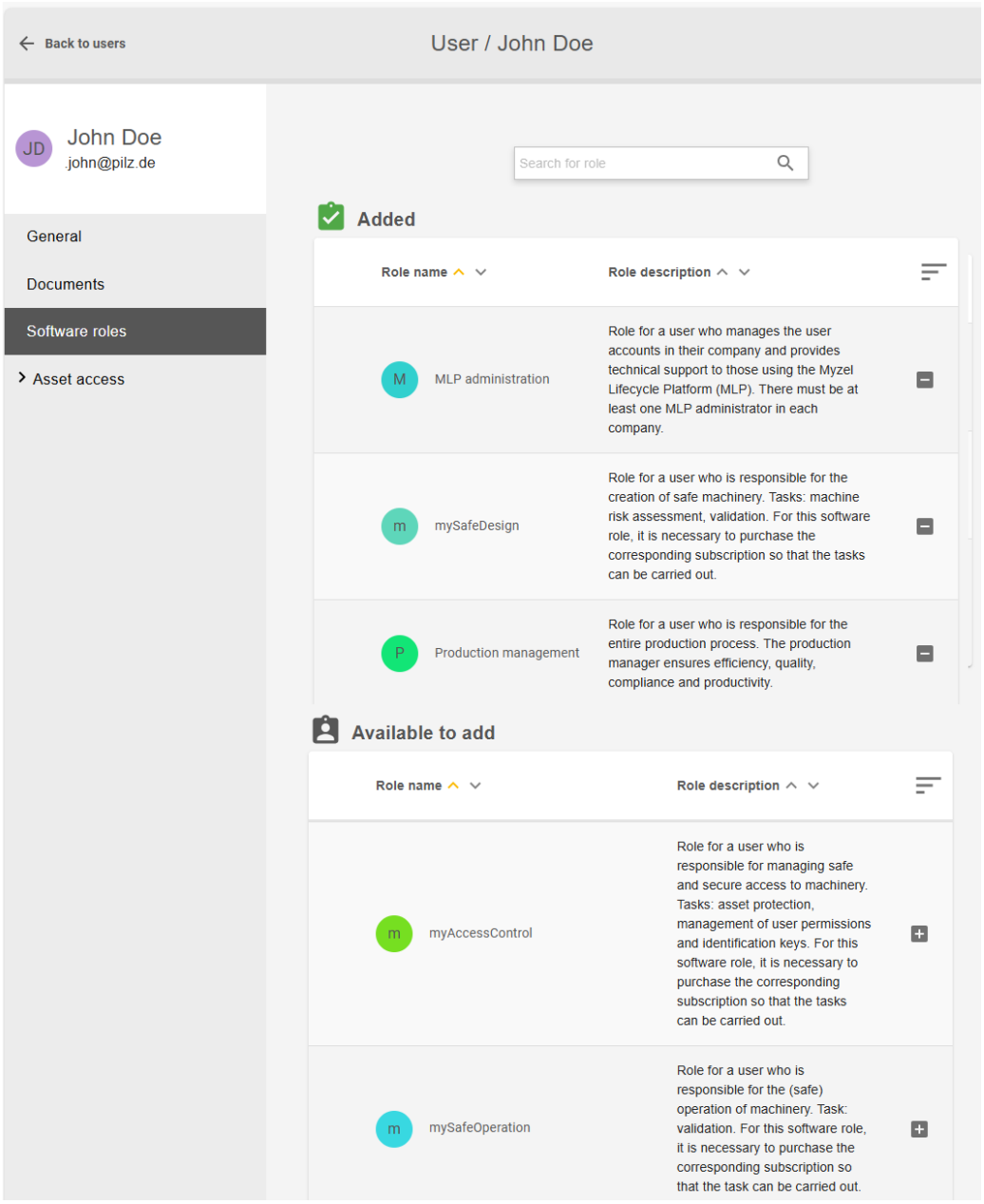
Procedure

1. Open Myzel Lifecycle Platform [📖 5].
2. Open user management
   ⇨ Select ***Manage users*** in the menu:



3. Assign software roles

   ⇨ Click on the user in the list of users. The user's profile is opened. On the Software roles tab, you can assign software roles to the user or remove assignments.



1.6 Manage subscriptions

Once the company account has been created for your company, the trial period begins. You can use the Myzel Lifecycle Platform for 30 days free of charge and try out all the functions.

By the time the trial period has ended, at the latest, you can choose between the following subscriptions:

- myCore
  Myzel platform module subscription to use the Myzel Lifecycle Platform.
  Functions included:
  - Management of assets, users and artifacts (digital artifacts are all types of files, such as documents, reports and certificates, for example)
  - Dashboards
  - Audit log

  This subscription is essential in order to use the platform. This subscription is available in various sizes. The size determines how many digital artifacts you can manage. You will be notified if you exceed this number.
- mySafeDesign
  Myzel workflow subscription for the creation of safe machinery.
  Function included:
  - Machine risk assessment
  - Design validation

  This subscription is available in various sizes. The size determines how many users can use the function concurrently. You will be notified if you exceed this number.
- mySafeOperation
  Myzel workflow subscription to (safely) operate machinery.
  Functions included:
  - Operational validation (inspection)

  The number of concurrent users is unlimited.
- myAccessControl
  Myzel workflow subscription to manage safe and secure access to machinery.
  Functions included:
  - Asset protection
  - Management of user permissions
  - Management of identification keys

  The number of concurrent users is unlimited.

1.6.1 Purchase subscription or change subscription size

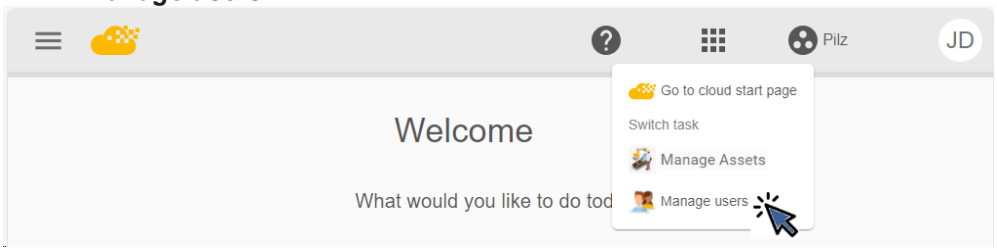
If you wish to purchase a new subscription or change the size of a subscription, because more users are to use a workflow at the same time for example, or you wish to store more digital artifacts, then you can do this directly in the Pilz E-Shop. However, it is more convenient if you start on the Myzel Lifecycle Platform. There you have an overview of your subscriptions and will be guided to the appropriate product in the E-Shop.

Prerequisites

- The action can be performed by users who have the following software role:
  - MLP administration

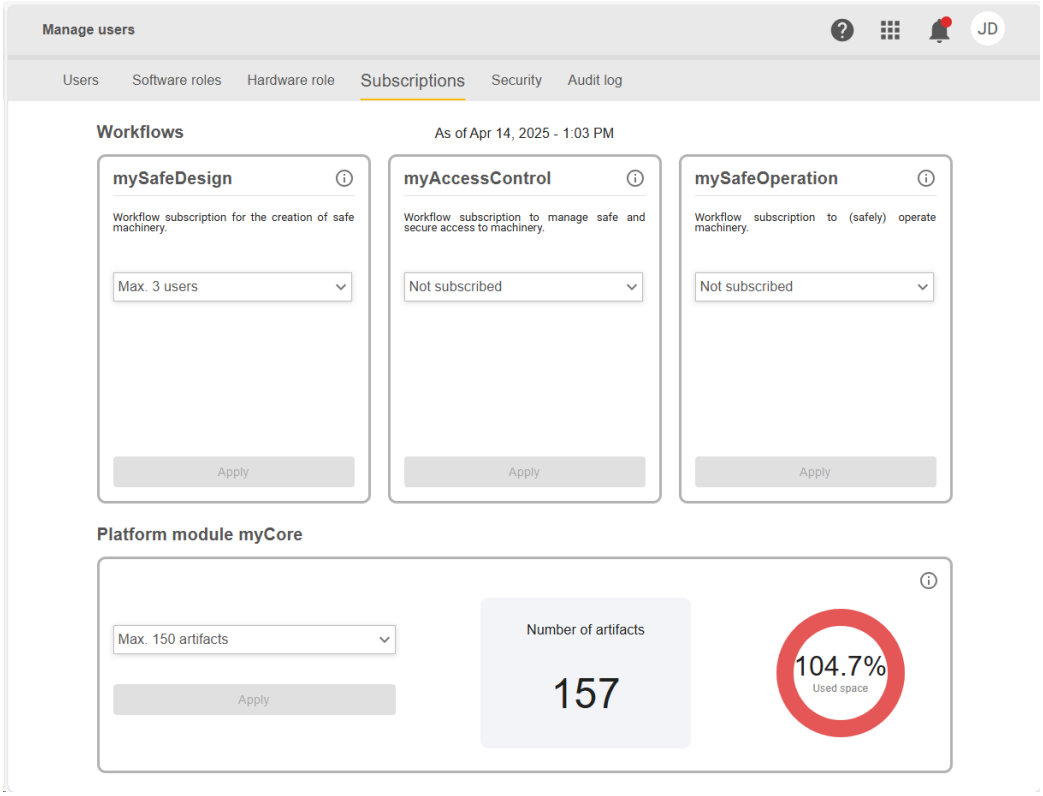
Procedure

1. Open Myzel Lifecycle Platform [5].
2. Open user management
   ⇨ Select ***Manage users*** in the menu:



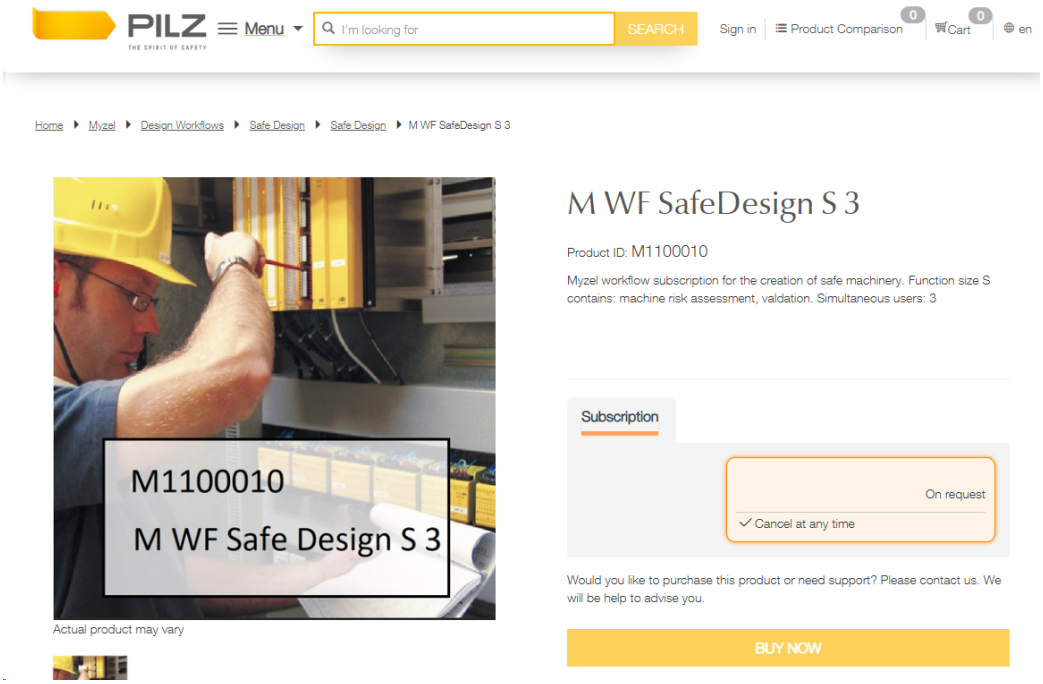
3. Select subscription

   On the ***Subscriptions*** page you can see which subscriptions you have currently purchased.



   ⇨ Select a subscription you have not yet subscribed to or change the size of a subscription and click ***Apply***.

The site for that product in the E-Shop is opened.



4. Purchase subscription in the E-Shop
   ⇨ Click on ***Buy now***.

You will soon receive a contract for the new subscription. As soon as you receive the contract, the subscription overview on the Myzel Lifecycle Platform is updated.

Notes

- Cancel subscription
  If you wish to cancel a subscription, please get in touch with your local Pilz contact (Locations - Pilz INT).

1.6.2 Cancel subscription

If you no longer wish to use a subscription, please get in touch with your local Pilz contact (Locations - Pilz INT).

2 Manage documents for users

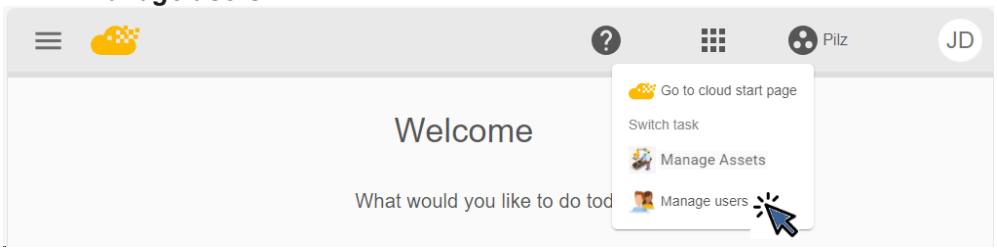
Documents for an employee, such as qualifications or work instructions, can be stored on the Myzel Lifecycle Platform. Alternatively you can link to a document that is stored in a different location.

Prerequisite

- The action can be performed by users who have the following software role:
  - MLP administration
  - myAccessControl
  - Production management

Procedure

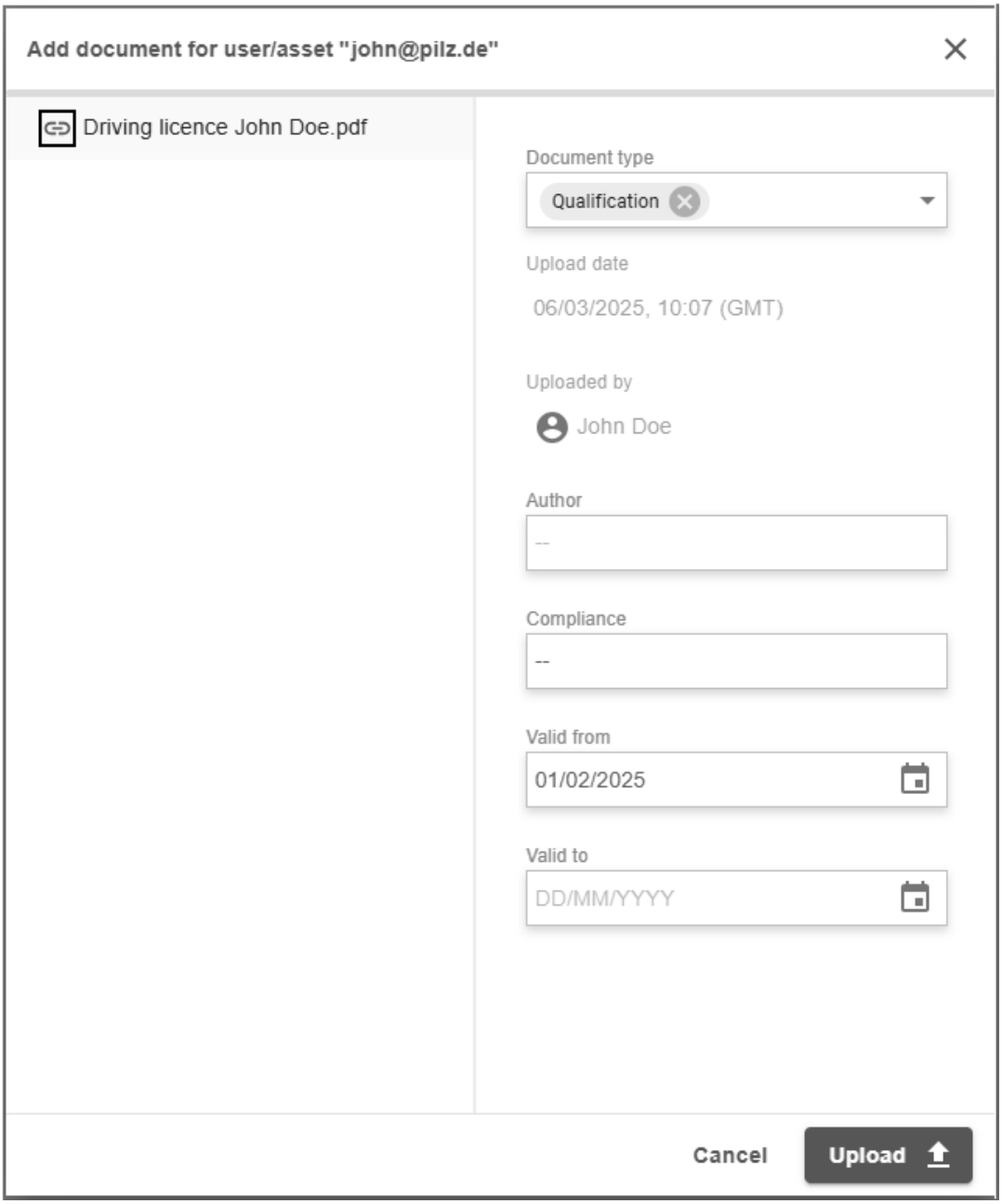
1. Open Myzel Lifecycle Platform [5].
2. Open user management
   ⇨ Select ***Manage users*** in the menu:



3. Manage documents
   ⇨ Double-click on the user. Switch to the ***Documents*** page in the user's profile.

Notes

Information can be entered for each document. Some of this metadata is used for the dashboards. More applications will follow in the future.


Add document for user/asset "john@pilz.de"
Driving licence John Doe.pdf
Document type
Qualification
Upload date
06/03/2025, 10:07 (GMT)
Uploaded by
John Doe
Author
--
Compliance
--
Valid from
01/02/2025
Valid to
DD/MM/YYYY
Cancel
Upload

3 Manage assets

In order to work with assets, they must be added to the Myzel Lifecycle Platform. Documents can then be saved for each asset and various actions can be performed, such as validations or risk assessments.

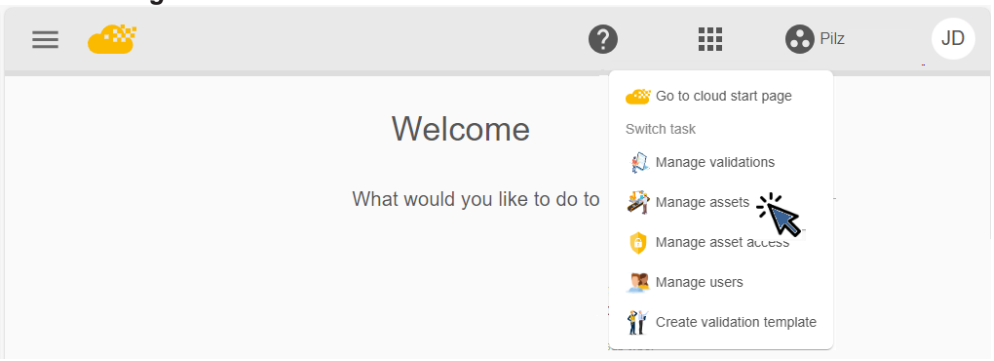
3.1 Open asset management

Prerequisite

- The action can be performed by all users. A software role is not required.

Procedure

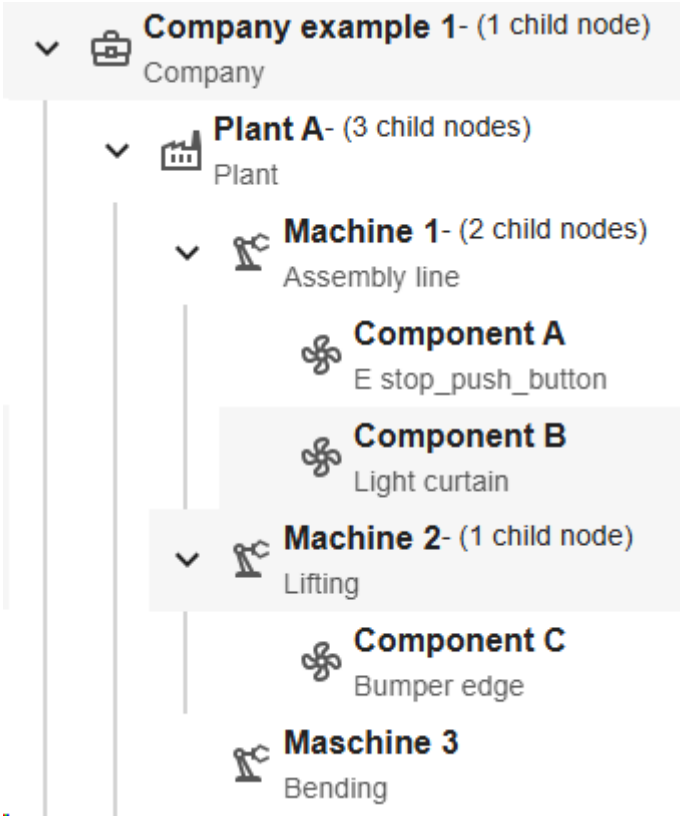
1. Open Myzel Lifecycle Platform [5].
2. Open asset management
   ⇨ Select ***Manage assets*** in the menu:



Asset management is opened.

3.2 Add assets

On the Myzel Lifecycle Platform there are various types of assets, such as company, plant, machine and component, for example. The assets can be organised in any tree structure.



Prerequisites

- The action can be performed by all users. A software role is not required.

Procedure

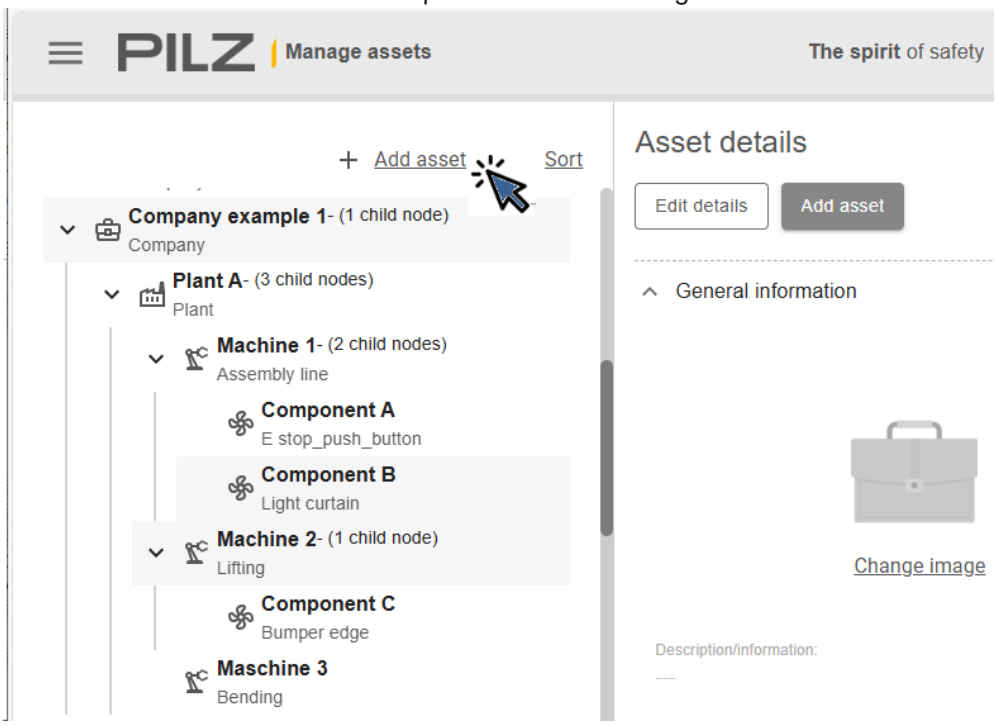
1. Open asset management

   See Open asset management [14].

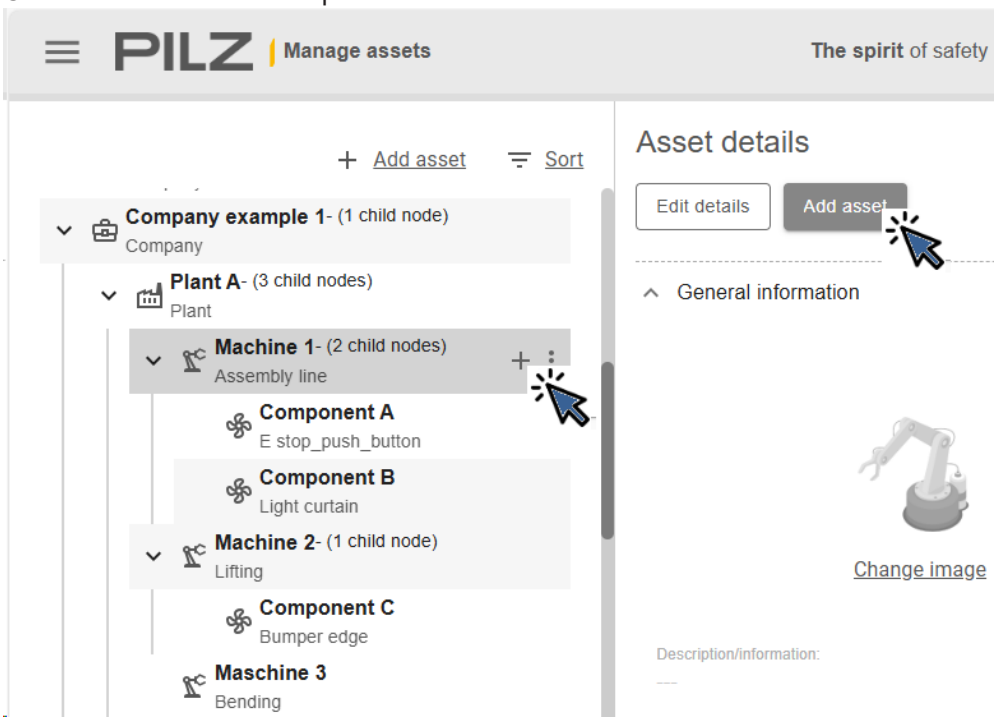
2. Add asset

   You must click in the right place, depending on where the asset is to be inserted in asset management.

– Click here to add the asset to the top level of asset management.



– Click in either of these two places to add the asset below another asset.



3. Enter the asset's details

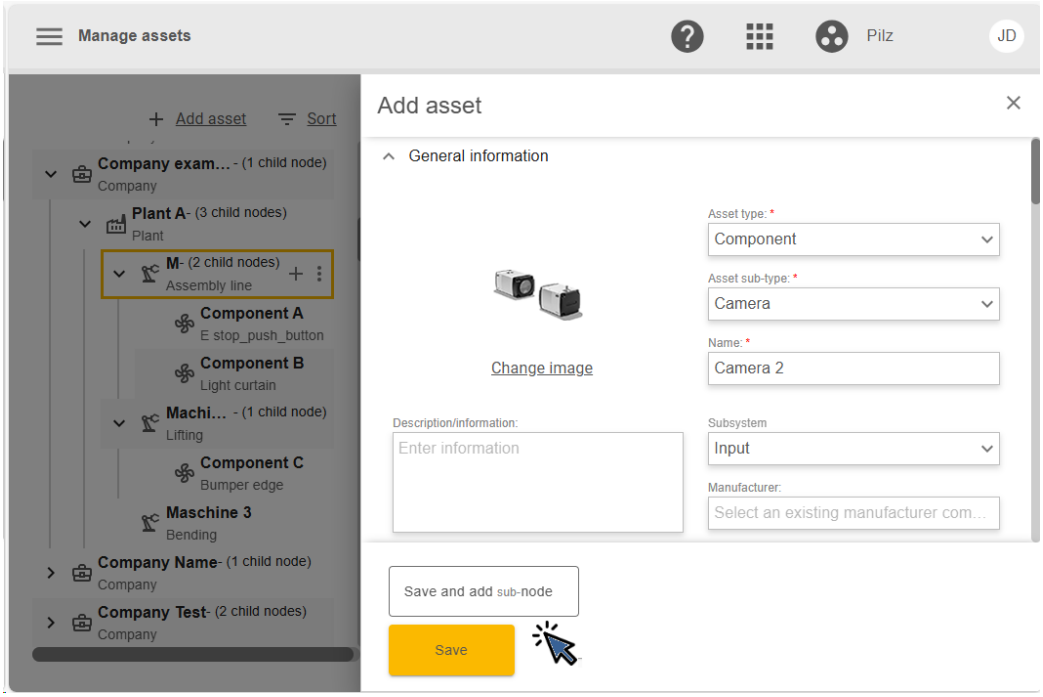
   You can enter the details for the new asset on the right-hand side. All fields with an * must be completed.

   ⇨ Enter the details of the new asset.

4. Complete the entry for the asset details

   When you have made all the entries you want, you can decide whether you only want to add this asset (***Save*** button) or also want to add the first subordinate asset (***Save and add sub-node*** button).

   ⇨ Click on ***Save*** or on ***Save and add sub-node***.



3.3 Transfer machine to another company account

A machine can be transferred from one company account on the Myzel Lifecycle Platform to another company account on the Myzel Lifecycle Platform. For example, if you are an OEM and have sold a machine, the machine data can be copied quite easily into your customer's company account.

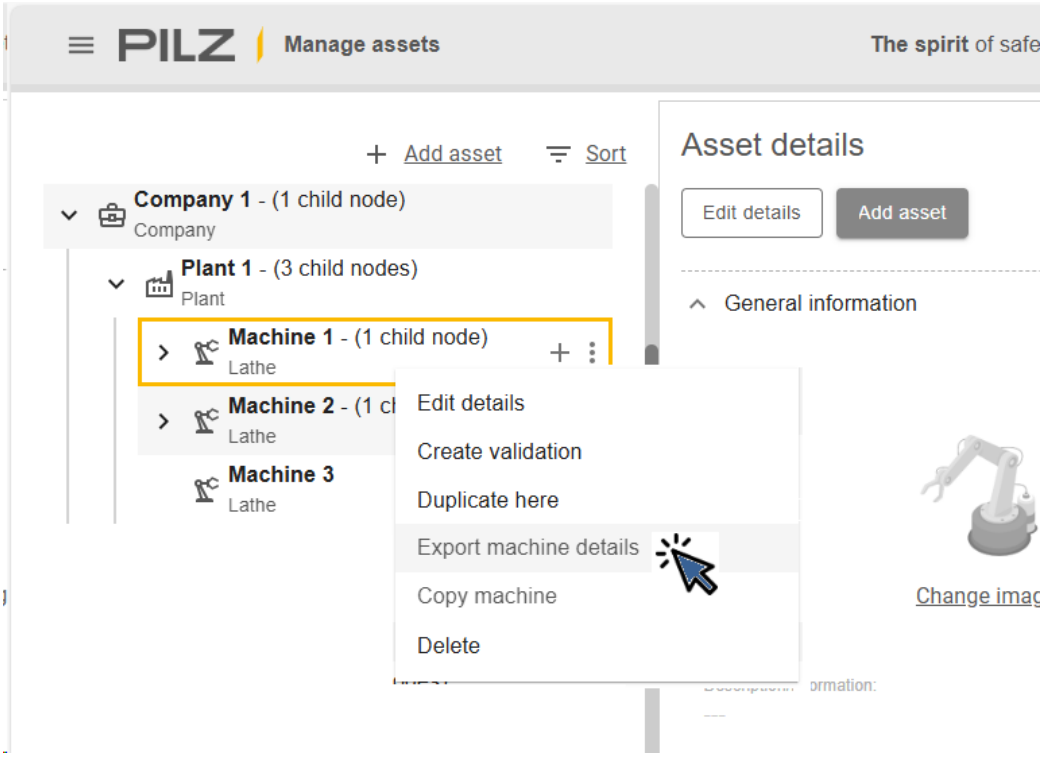
INFORMATION

At the moment, only a machine's details can be transferred to another company account. Soon it will be possible to transfer all the machine's documents, completed validations and risk assessments (PDF files of the reports).

Procedure

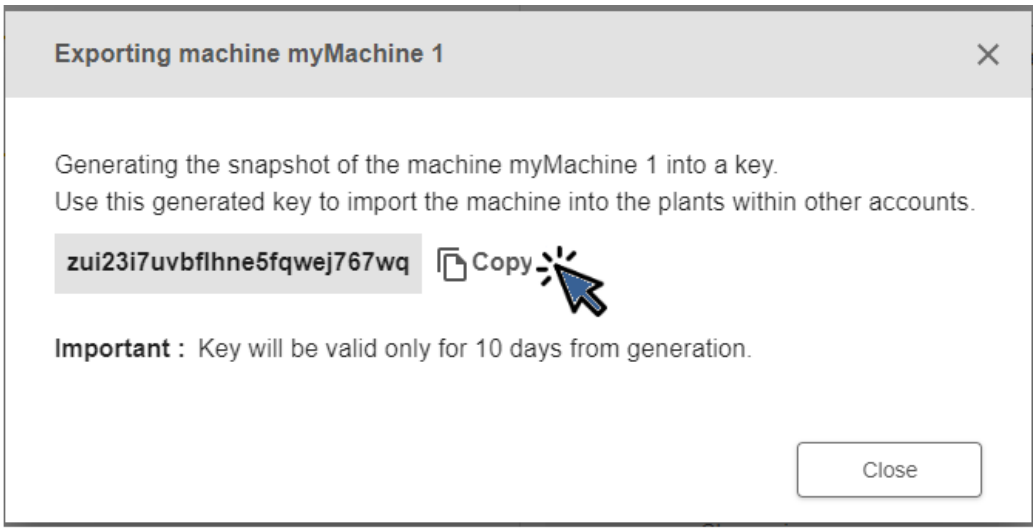
1. Select machine

   ⇨ In the asset view, navigate to the machine that is to be transferred, open the menu for the machine (⋮ icon) and select ***Export machine details***.



2. Copy key

   ⇨ Copy the key and send the key to a person with access to the other company account.



3. Import machine

   The person who has received the key can now import the machine. They must proceed as follows:

   ⇨ The person must navigate to the asset to which the machine is to be added and click on ***Import machine***. The person can then enter the key.

The machine is inserted at the selected point.

4 Validate assets

On the Myzel Lifecycle Platform, the validation of plant and machinery (including components) can be carried out using predefined validation templates. It is not possible to validate other asset types.

INFORMATION

There are operational validations (inspections) and design validations. The type of validation a user is allowed to perform depends on the assigned software role (mySafeOperation, mySafeDesign).

4.1 Prepare a machine's validation

To enable a validation to be performed, a validation template must be selected and the validation created.

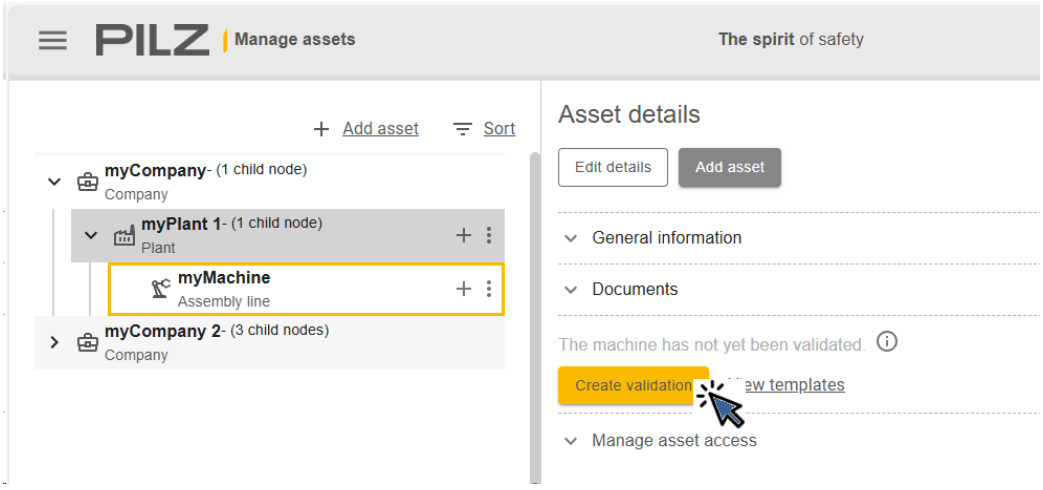
Prerequisites

- The action can be performed by users who have the following software role:
  - mySafeDesign
  - mySafeOperation
- The machine is available in asset management (see Add assets [15]).

Procedure

1. Select machine

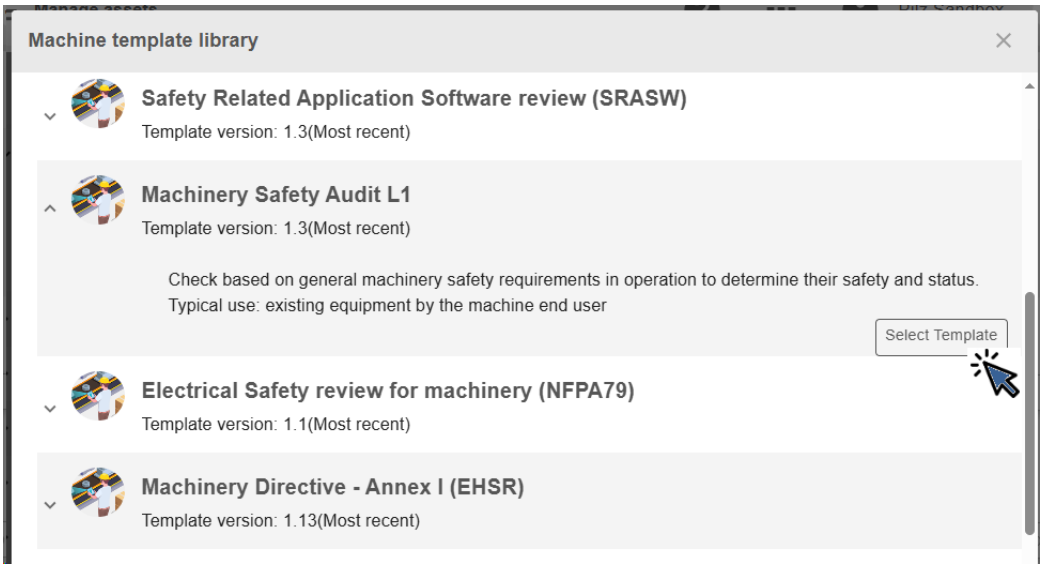
   ⇨ In asset management, navigate to the required machine and click on ***Create validation***.



2. Select validation template

   Validation templates contain predefined lists of questions.

   ⇨ Select a template from the ***Validation template*** field. If you need explanations of the validation templates, click on ***View templates***. The ***Machine template library*** is opened. When you have found the right validation template in the ***Machine template library***, click on ***Select template*** in the description of the validation template.



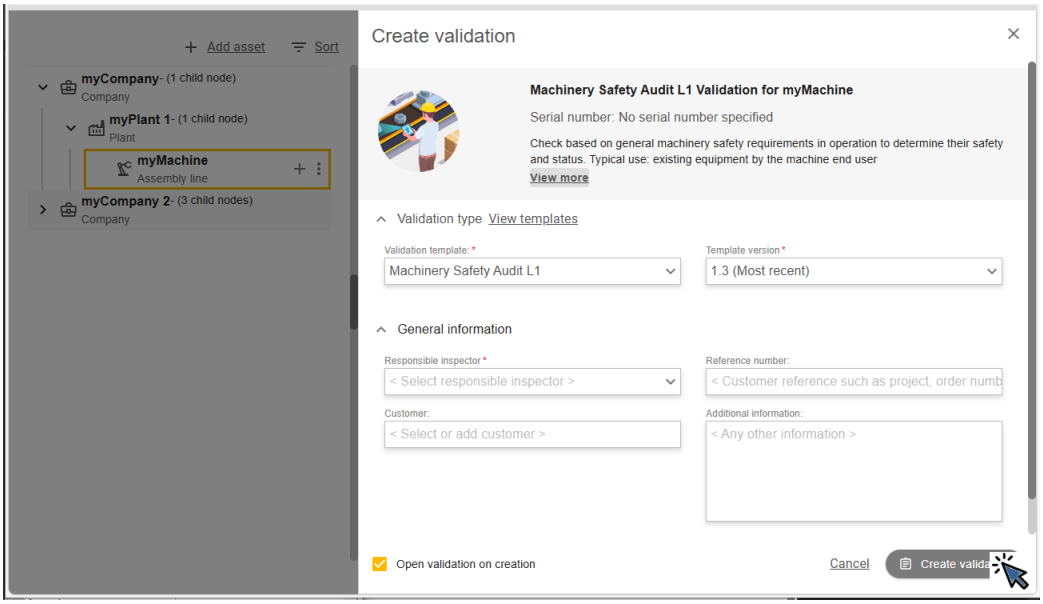
3. Select version of validation template

   Different versions of the validation templates may be available. Pilz recommends that you always use the latest version.

   ⇨ Select the required version in the ***Template version*** field.

4. Create validation

   ⇨ Click on ***Create validation***.

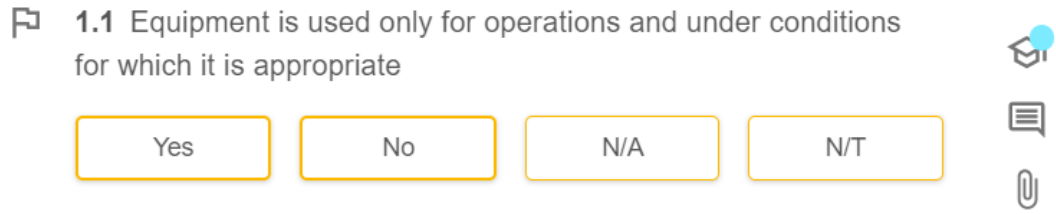


The validation template is opened and you can start answering the questions immediately. See Perform validation [📖 21].

4.2 Perform validation

All the questions on the validation template must be answered during validation.

Structure of a question:



The following answers are possible:

- ***Yes***
  Condition is met.
- ***No***
  Condition is not met.
- ***N/A*** (Not applicable)
  The question is not applicable to the machine/component.
- ***N/T*** (Not testable)
  The question cannot be tested on the machine/component.

Meaning of the icons on the right-hand side:

-  Knowledge database
  A knowledge database is available to support you in answering the questions. It contains information and explanations regarding the questions. When there is information about a question in the knowledge database, the icon is marked with a blue dot (as shown). Click on the icon to view the information.

-  Comment
  A comment can be entered for each question. Click on the icon to enter a comment. If the icon is marked with a blue dot, then a comment is available.

-  Picture
  A picture (*.jpeg, *.jpg, *.png) can be added to each question. Click on the icon to add a picture. If the icon is marked with a blue dot, then a picture is available.

Flag:

Questions can be marked with a red or blue flag. Questions that are marked with a flag are easy to find and edit later. Always add a comment to questions with a flag, to inform the inspector about the reasons for the answer.

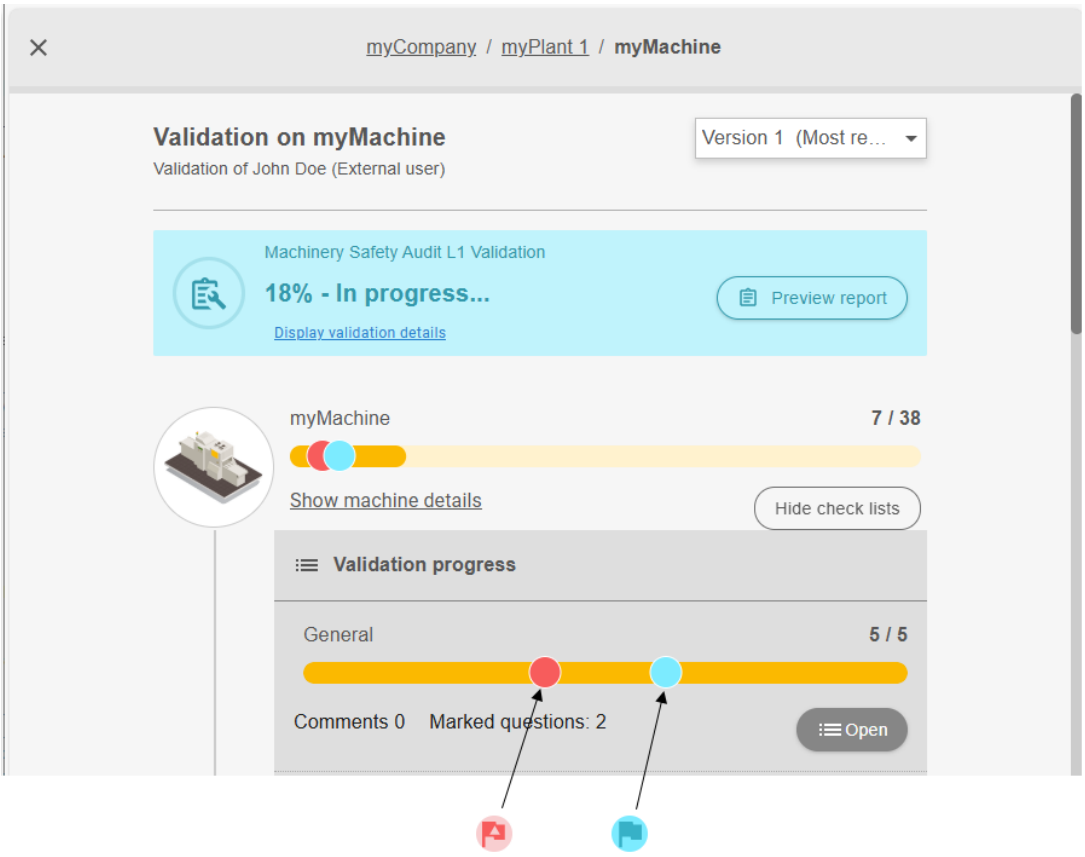
-  Red flag
  Questions to which the answer is no are automatically given a red flag. The red flag cannot be removed manually.

- Blue flag

  Questions that are answered with N/T are automatically given a blue flag. The blue flag can also be set manually, to mark the question for editing later, for example, or to show that the question has a comment.

  Click on the flag icon to set or remove the blue flag.

Questions that are marked with a flag are also displayed in the validation status:



Clicking on the dot takes you directly to the relevant question.

Prerequisites

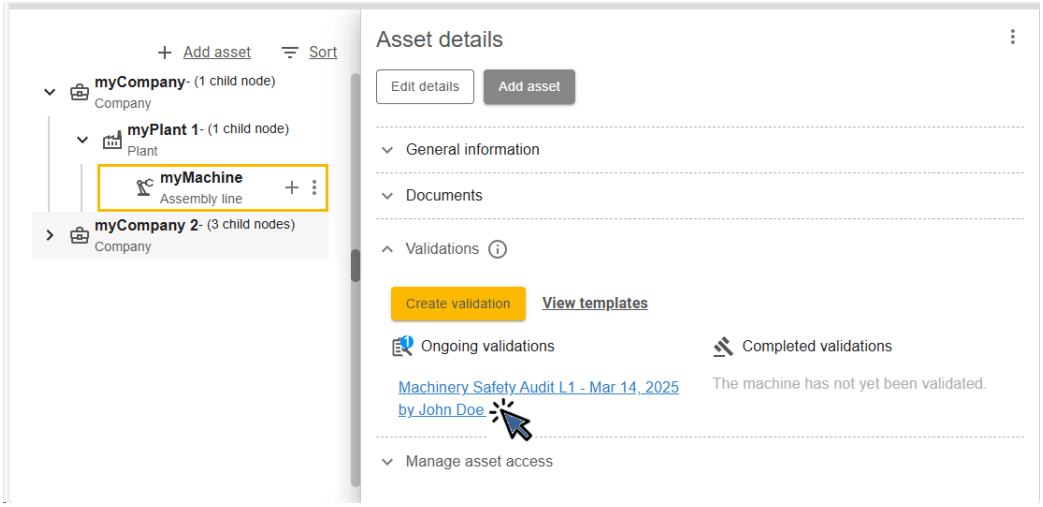
- The action can be performed by users who have the following software role:
  - mySafeDesign
  - mySafeOperation
- The validation has been created (see Prepare a machine's validation [📖 19]).

Procedure

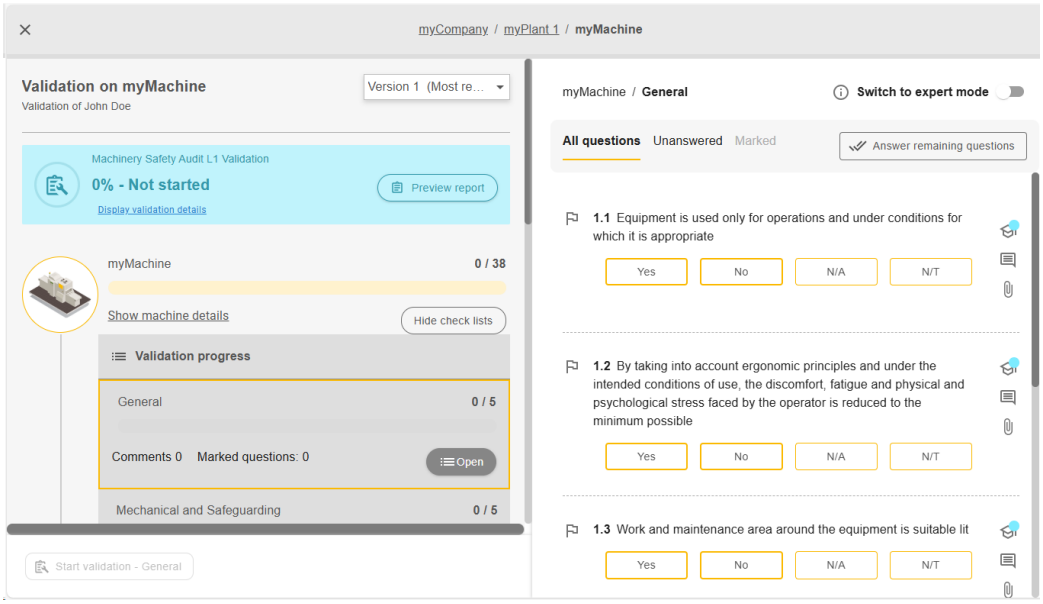
1. Select validation

   If the list of questions is not yet open, follow the instructions below:

   ⇨ In asset management, navigate to the machine that is to be validated and click on the required validation in the asset details.



The list of questions is opened. The left-hand side of the screen shows the status of the validation and the right-hand side shows the questions for the validation.



2. Answer questions

   The questions can now be answered.

   ⇨ Answer the questions.

All answers are saved automatically.

When all the questions have been answered, the validation can be completed. See Complete validation [📖 24].

4.3 Complete validation

When all the questions have been answered, the validation can be completed.

Prerequisites

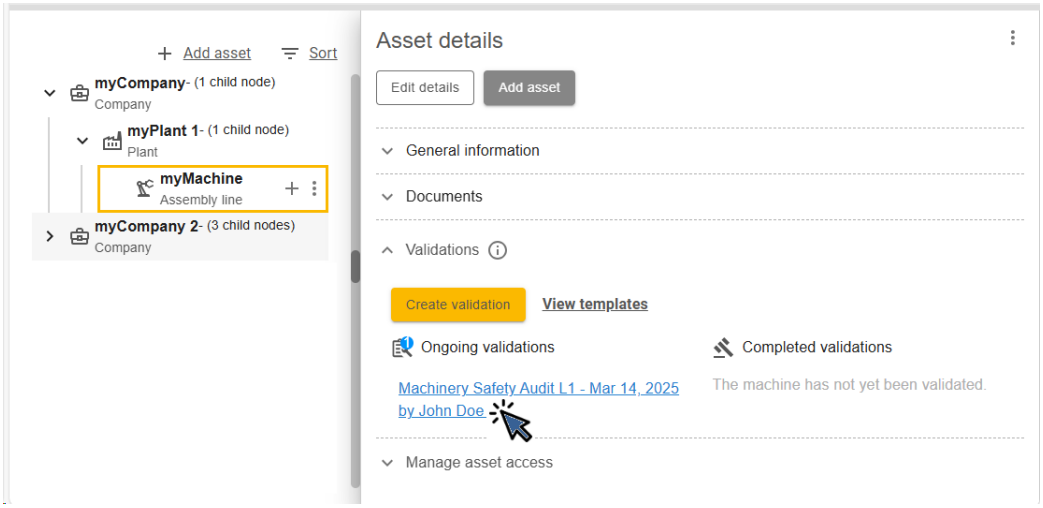
- The action can be performed by users who have the following software role:
  - mySafeDesign
  - mySafeOperation

Procedure

1. Select validation

   If the validation is not yet open, follow the instructions below:

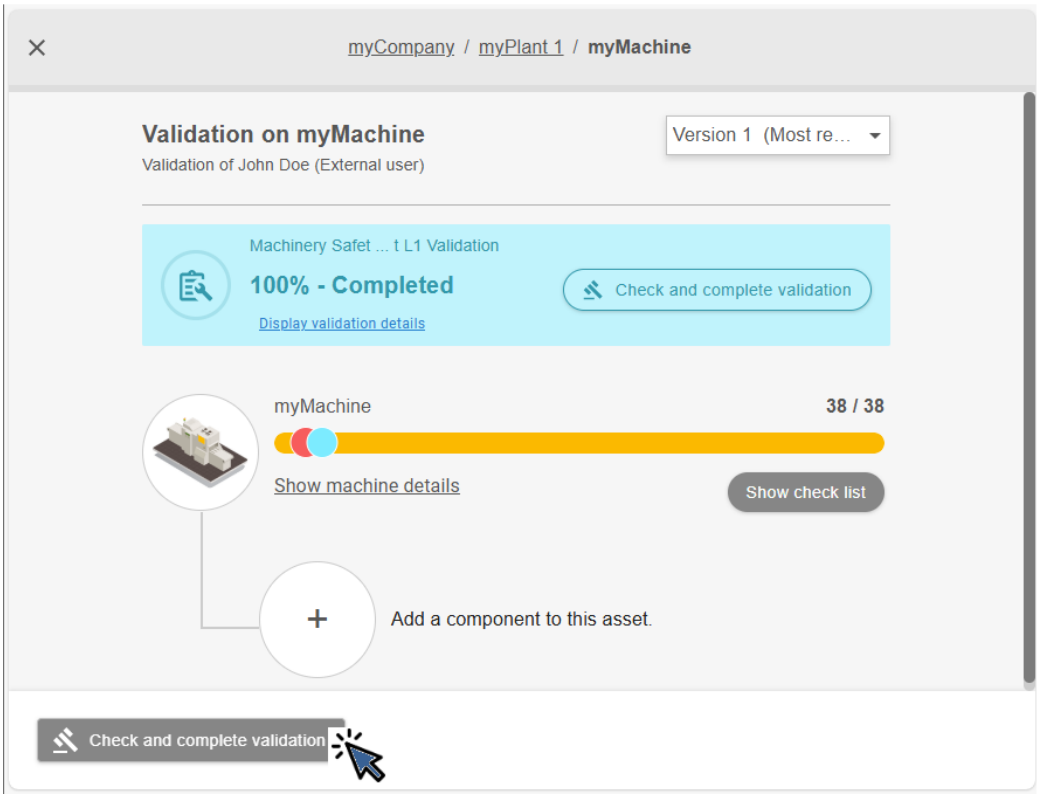
   ⇨ In asset management, navigate to the machine whose validation is to be completed and click on the required validation in the asset details.



   The list of questions is opened. The status of the validation is displayed.

2. Start action

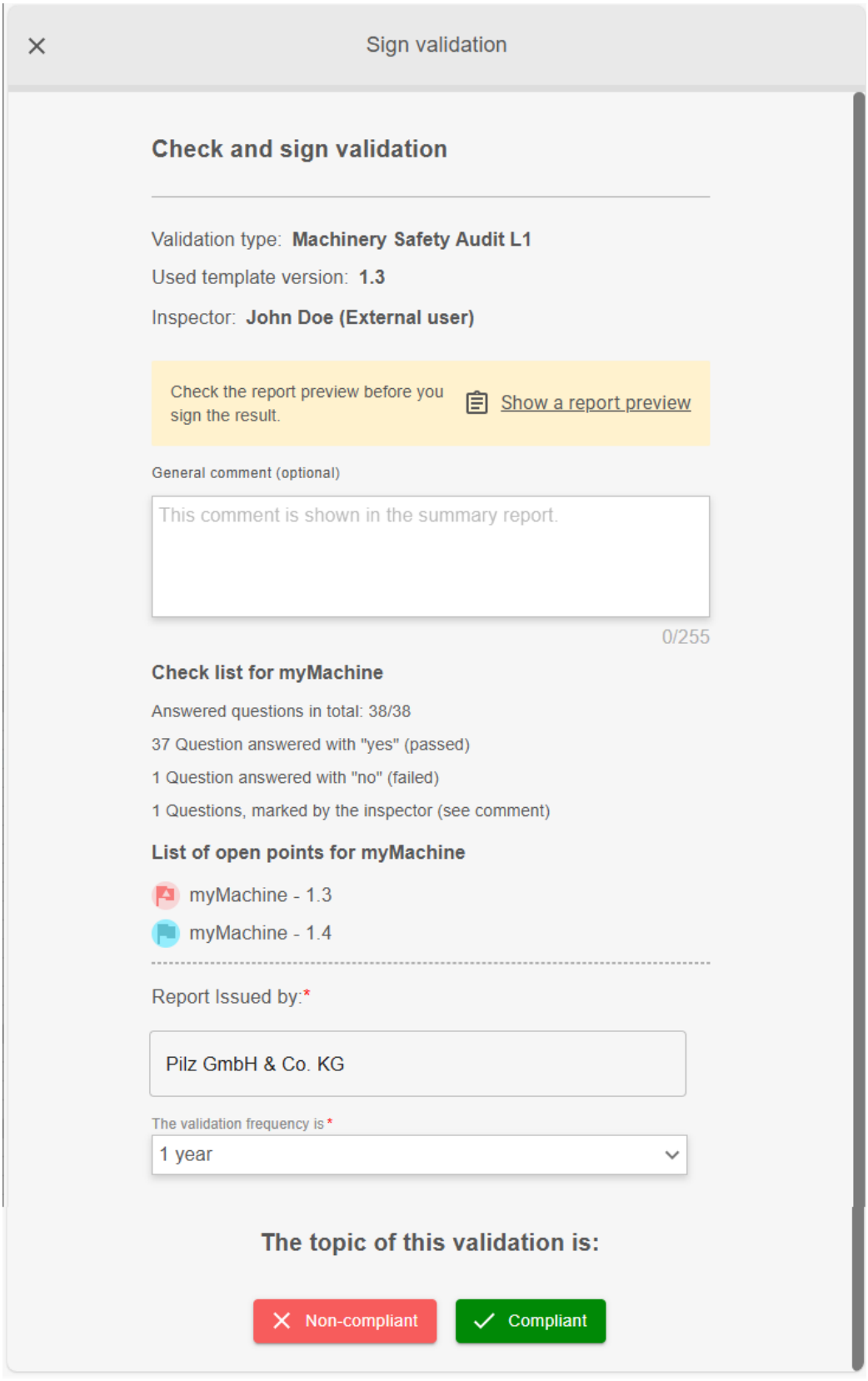
   When all the questions have been answered, the status is "100% - Completed".



⇨ Click on ***Check and complete validation***.

3. Check validation

   You will see a summary of the validation and can display a preview of the report.



⇨ Check the answers to the questions carefully, complete the field ***Report Issued by*** and then click on ***Compliant*** or ***Non-compliant***.

The validation is completed and versioned. You can create a full report of this validation, which contains detailed information about the machine and the questions. To do this, click on ***Open report***.

You can edit a completed validation at any time, to answer any open questions in a non-compliant validation for example. See Correct validation [📖 27].

If an asset needs to be re-validated, you can carry out the validation again, based on the existing validation. See Re-validate [📖 28].

Notes

- Overview of validations
  If you highlight an asset in asset management and select ***Manage validations*** in the  menu, an overview of all the validations for the asset is displayed. You can view and edit the validations.
  To create a report of all validations, or validations selected from the list, click on ***Create overall report***. The overall report can be saved as an Excel file (*.csv) or as a PDF file.
- Deletion of assets
  An asset for which a completed validation is available can no longer be deleted from the MLP.

4.4 Correct validation

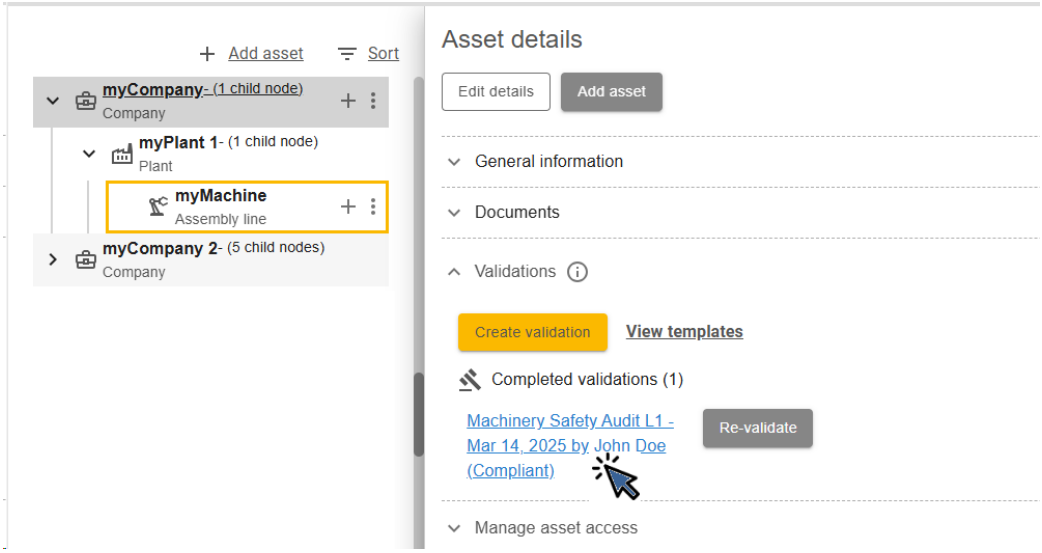
A completed validation can be corrected, if an error has been found in a validation for example. A new version of the existing validation is created in the process. All the answers in the validation are retained and can be amended.

Prerequisites

- The action can be performed by users who have the following software role:
  – mySafeDesign
  – mySafeOperation

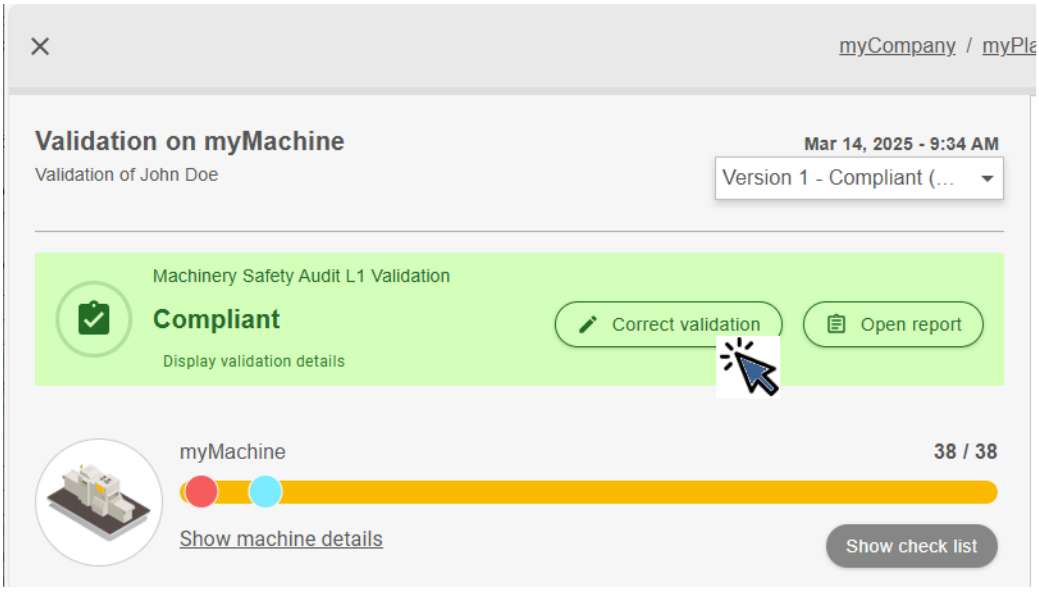
Procedure

1. Select validation
   ⇨ In asset management, navigate to the asset for which the validation was created and click on the validation you wish to correct.



2. Start correction

   ⇨ Click on ***Correct validation***.



A new version of the validation is created. You can now correct the answers.

4.5 Re-validate

A completed validation can be re-validated. The questions and answers from the already completed validation can be copied in the process. When a validation is re-validated, a new validation is created, with version 1.

Prerequisites

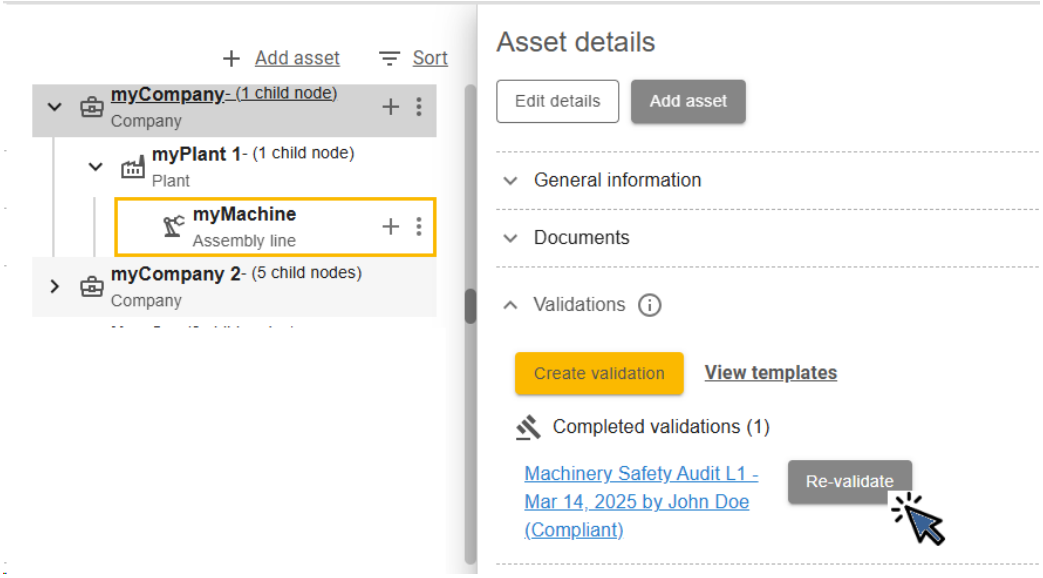
- The action can be performed by users who have the following software role:
  - mySafeDesign
  - mySafeOperation
- When the validation template was created, it was configured to allow re-validation. Not all validations can be re-validated.

- There have been no major changes to the validation template since the validation was completed. The first digit of the version number of the validation template must not have changed, from 2.1 to 3.0 for example.

Procedure

1. Select validation

   ⇨ In asset management, navigate to the asset for which the validation was created and click on ***Re-validate*** next to the required validation.



   If there is no ***Re-validate*** button, then the validation cannot be re-validated (see pre-requisites above).

2. Copy answers

   You can decide whether to copy the answers from the existing validation.

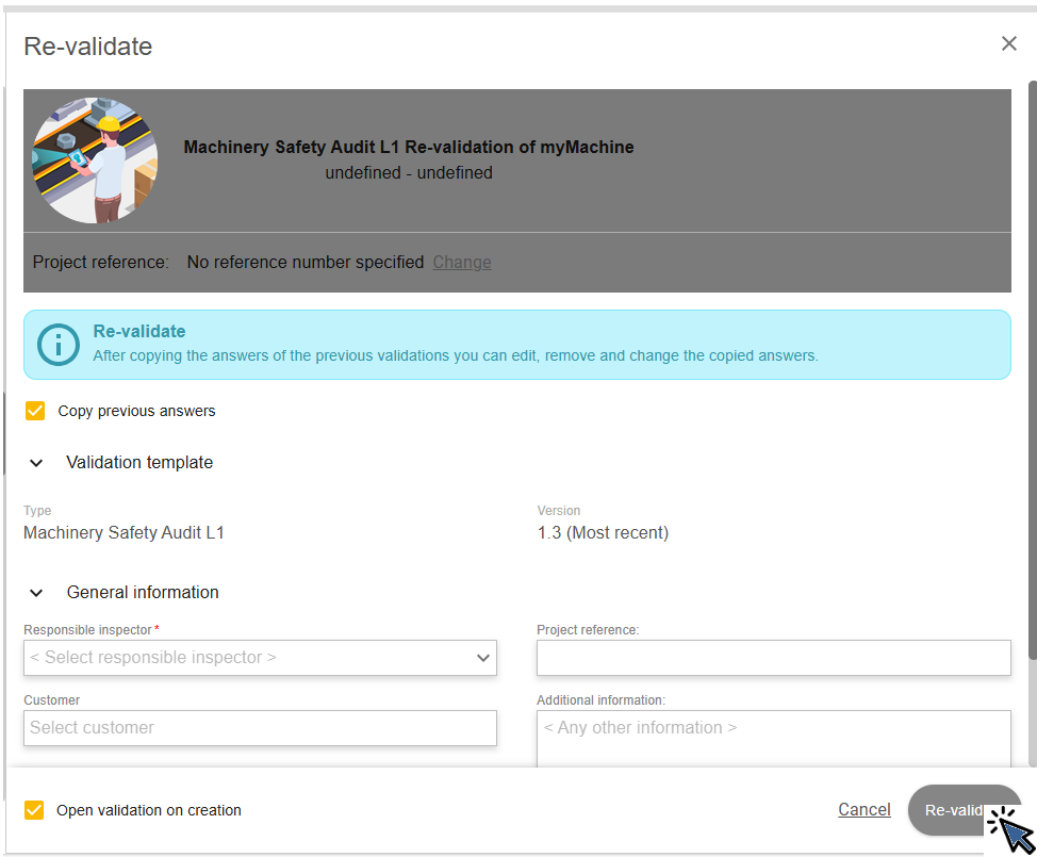
   ⇨ If required, tick the ***Copy previous answers*** option.

3. Decide about the list of questions

   ⇨ Untick the ***Open validation on creation*** option if the list of questions is not to be opened after the validation is created.

4. Start re-validation

   ⇨ Click on ***Re-validate***.



A new validation is created and the questions can be answered.

5 Create risk assessment

A machine risk assessment can be created on the Myzel Lifecycle Platform.

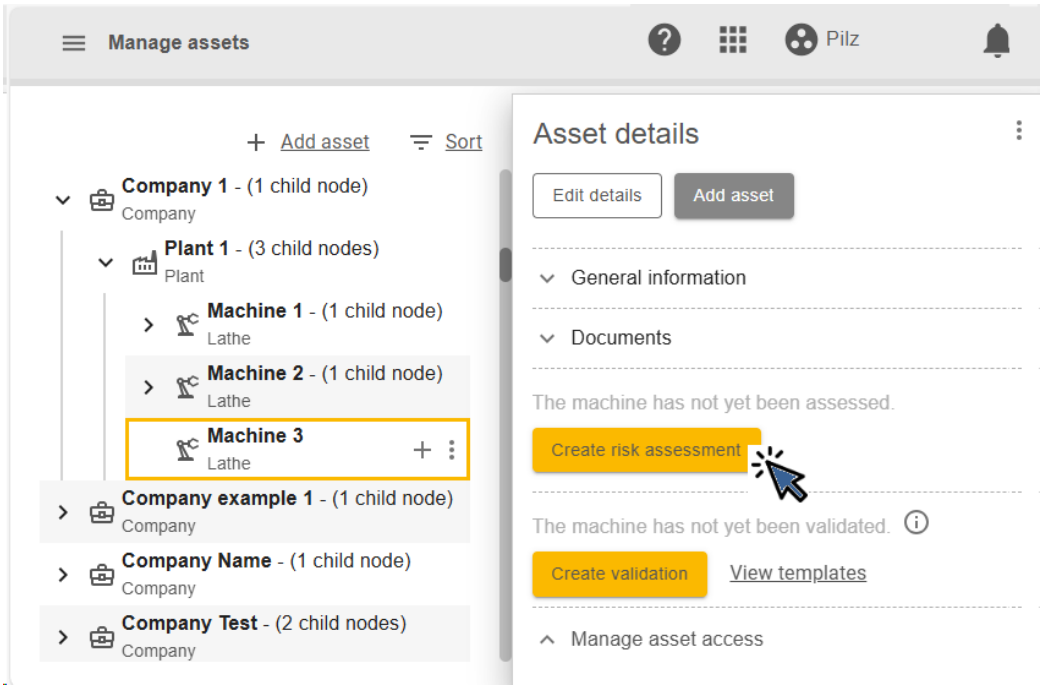
In accordance with EN ISO 12100, risk assessment is described as an iterative process to minimise risk. Each hazard must be systematically examined separately under its operating conditions. Risk-reducing measures must then be implemented using the 3-step iterative process from EN ISO 12100 – Clause 6 until the risk has been eliminated or sufficiently reduced.

Prerequisites

- The action can be performed by users who have the following software role:
  - mySafeDesign
- The machine is available in asset management (see Add assets [📖 15]).

Procedure

➪ In asset management, navigate to the required machine and click on ***Create risk assessment***.



6 Manage asset access

Not all users may perform all actions on all machines. A PITreader can be assigned to a machine in order to manage user access rights. This PITreader can be used to authenticate and authorise users. The authorisation can be evaluated using a safe evaluation unit (e.g. PIT m4SEU) or a control system.

All machines for which the same access rules should apply are combined into a protected asset group.

The configuration for PIT UAS can be carried out on the MLP, and it is possible to determine the permissions and user data that apply to a transponder/user. The data must be transferred from the MLP to the PIT UAS. The data is then evaluated outside of the MLP.

MLP has a dashboard, which provides an overview of the protection of assets and users.

Note for PITreader users:

Term on PITreader	Term on MLP
Device group	Protected asset group
Permission	Hardware permission
Transponder	Identification key

The following actions are required to manage asset access. There is no specified order for the actions, but some actions require data from other actions. We recommend the following order:

- Add assets to asset management
  All machines that are to be protected must be added to asset management.
  See Add assets [📖 15].
- Create asset group
  All machines for which the same access rules should apply must be combined into a protected asset group.
  See Create asset group [📖 34].
- Assign PITreader
  A PITreader must be assigned to each machine that is to be protected.
  See Assign PITreader [📖 37].
- Configure and use PITreader user data
  Information about a user (e.g. language, user name, ...) can be stored in the PITreader user data; this information should be retrievable by the PIT UAS.
  See Configure and use PITreader user data [📖 40].
- Assign hardware permissions to users
  On the MLP it is possible to determine the hardware permissions that apply to a user/transponder.
  See Assign hardware permission to users [📖 41].
- Assign identification key to users
  Exactly one identification key must be assigned to each user.
  See Assign identification key to users [📖 44].

- Edit asset group numbers
  Each asset group has a name on the MLP. The PITreader does not know these names, but works with numbers for the device groups.
  See Edit asset group numbers [📖 44].
- Define numbers for hardware permissions
  The hardware permissions that are to be used for an asset group are defined. Each hardware permission has a name on the MLP. The PITreader does not know these names, but works with numbers for the permissions.
  See Define numbers for hardware permissions [📖 46].
- Sync data with PIT UAS
  The configuration for PIT UAS can be carried out on the MLP. Whenever the configuration has changed, the data must be transferred again from the MLP to the PIT UAS.
  See Sync data with PIT UAS [📖 47].

6.1 Open access management

There is a dashboard with an overview and a central menu for managing asset access. All important actions can be started in the menu.

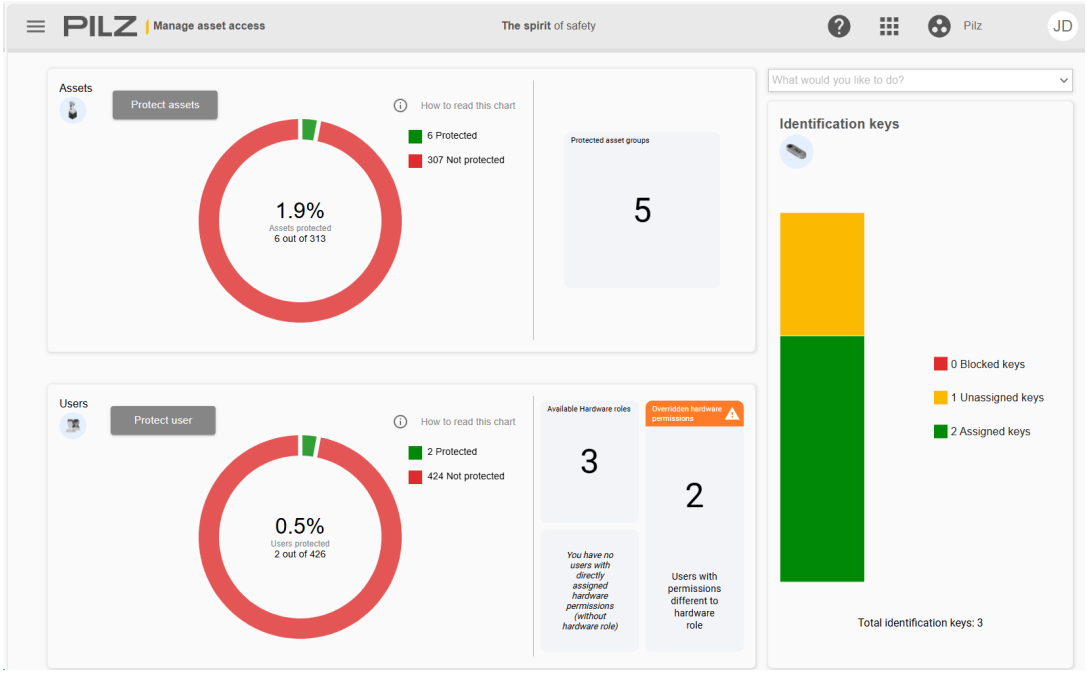
Prerequisites

- The action can be performed by users who have the following software role:
  – myAccessControl

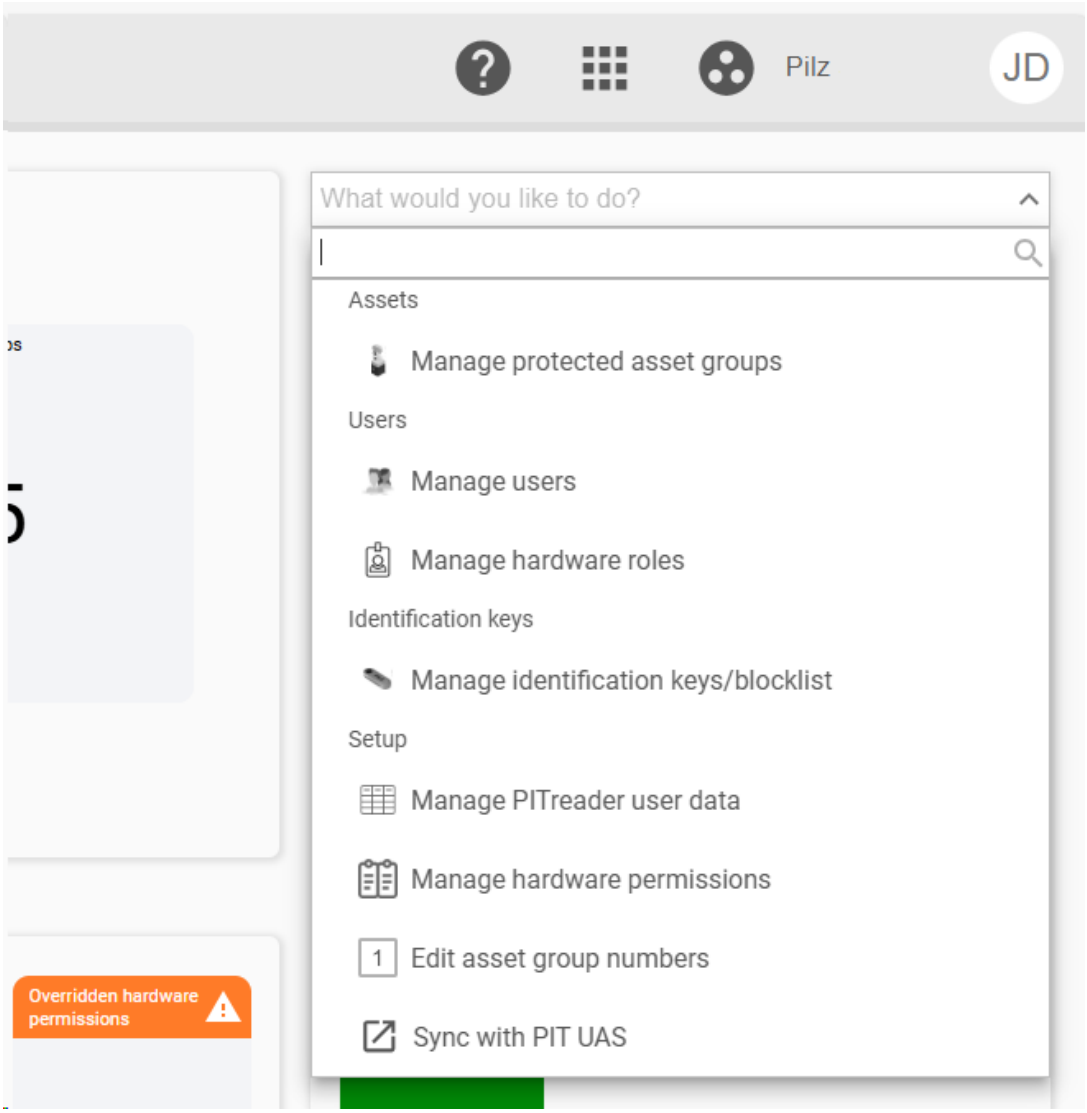
Procedure

⇨ Select ***Manage asset access*** from the  menu.

The access management dashboard is displayed.



The central menu is located top right.



6.2 Create asset group

All machines for which the same access rules should apply must be combined into a protected asset group.

Prerequisites

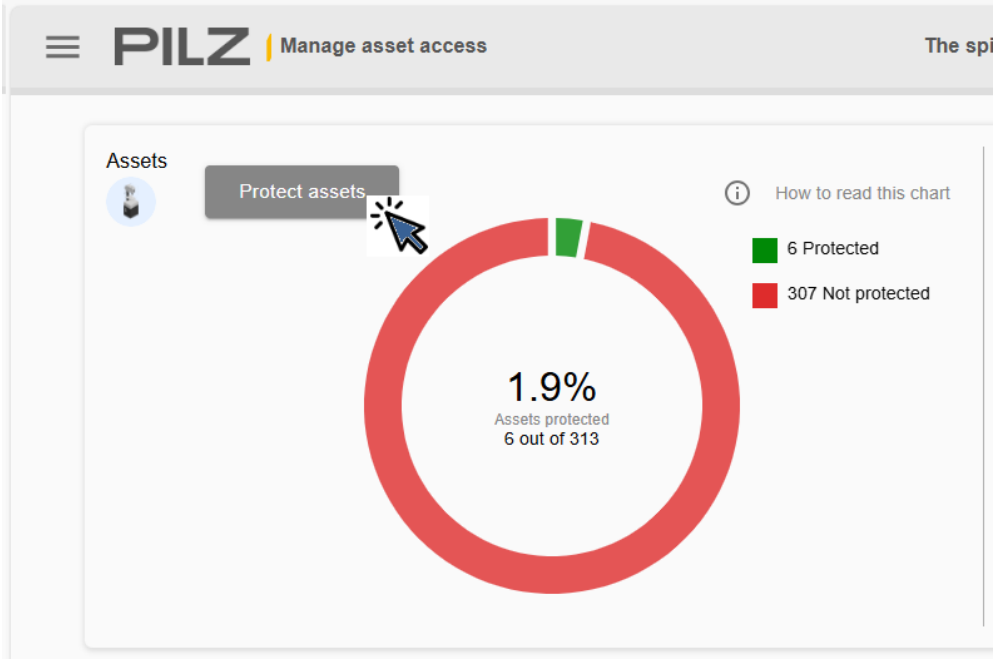
- The action can be performed by users who have the following software role:
  - myAccessControl
- The machines are available in asset management (see Add assets [15]).

Procedure

1. Open access management

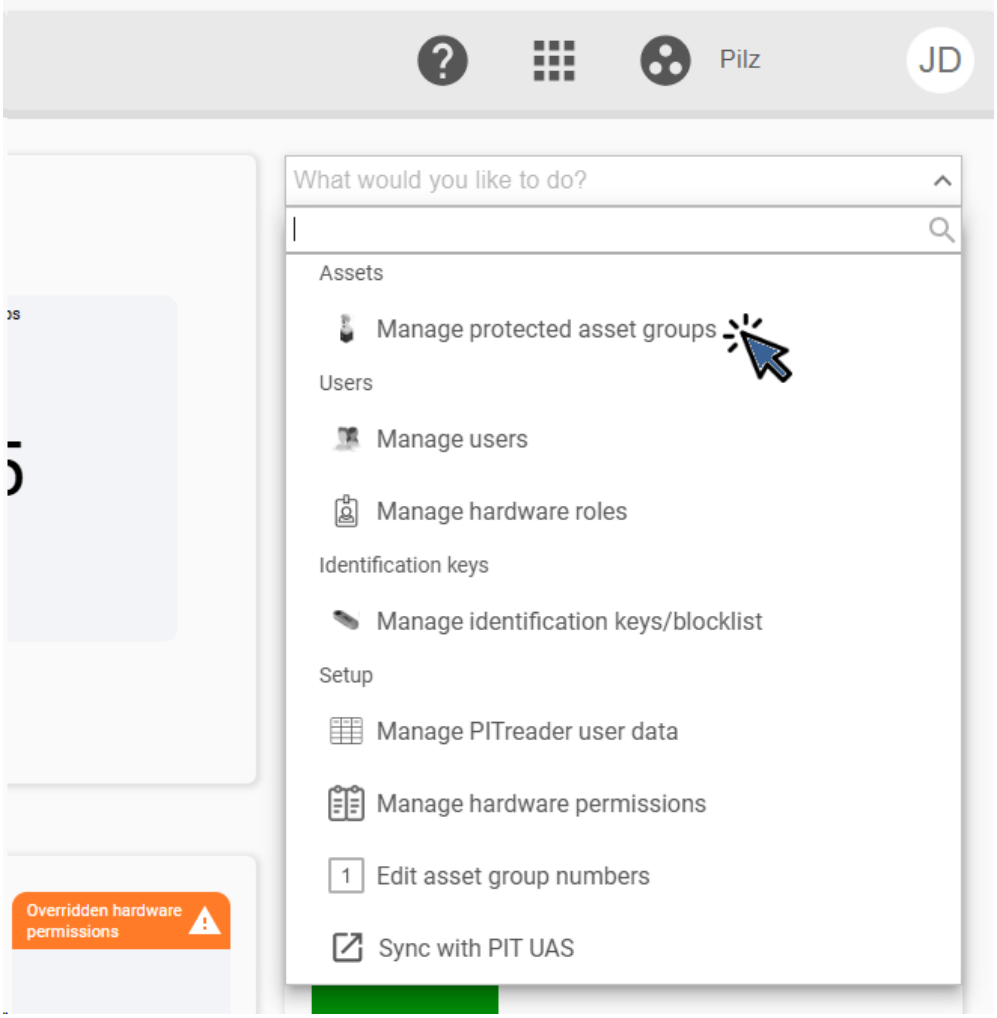
   See Open access management [33].

2. Start action
   There are three options for starting the action.
   Option 1:
   ⇨ Click on ***Protect assets***.



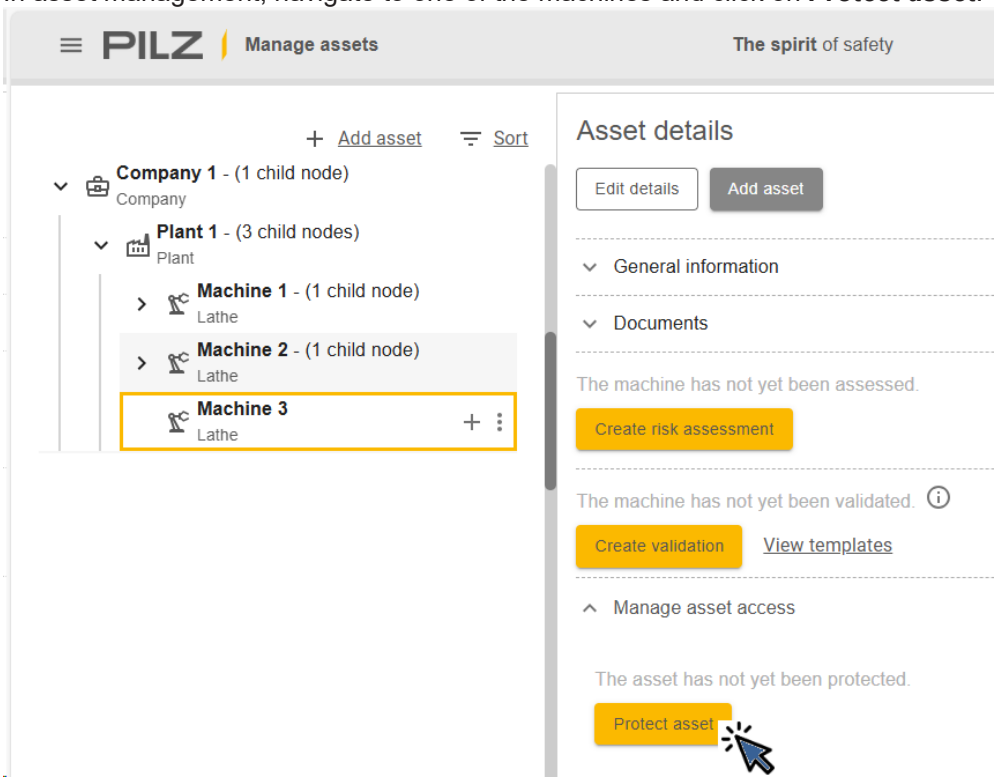
Option 2:

⇨ In the access management menu, select ***Manage protected asset groups*** and then click on ***Add protected asset group***.



Option 3:

➪ In asset management, navigate to one of the machines and click on ***Protect asset***.



3. Perform steps

   You will be guided through the steps required to create an asset group.

   ➪ Follow the instructions.

The asset group is created.

6.3 Assign PITreader

A PITreader must be assigned to each machine that is to be protected.

There are three methods for assigning a PITreader to a machine.

Method 1

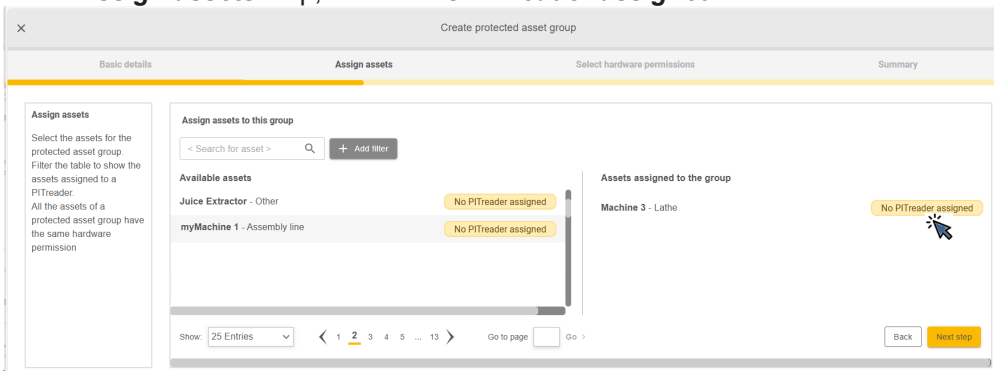
The PITreader is added to a machine when the asset group is created. This is the simplest method.

1. Create asset group

   ➪ See Create asset group [📖 34].

2. Add PITreader

⇨ In the ***Assign assets*** step, click on ***No PITreader assigned***.

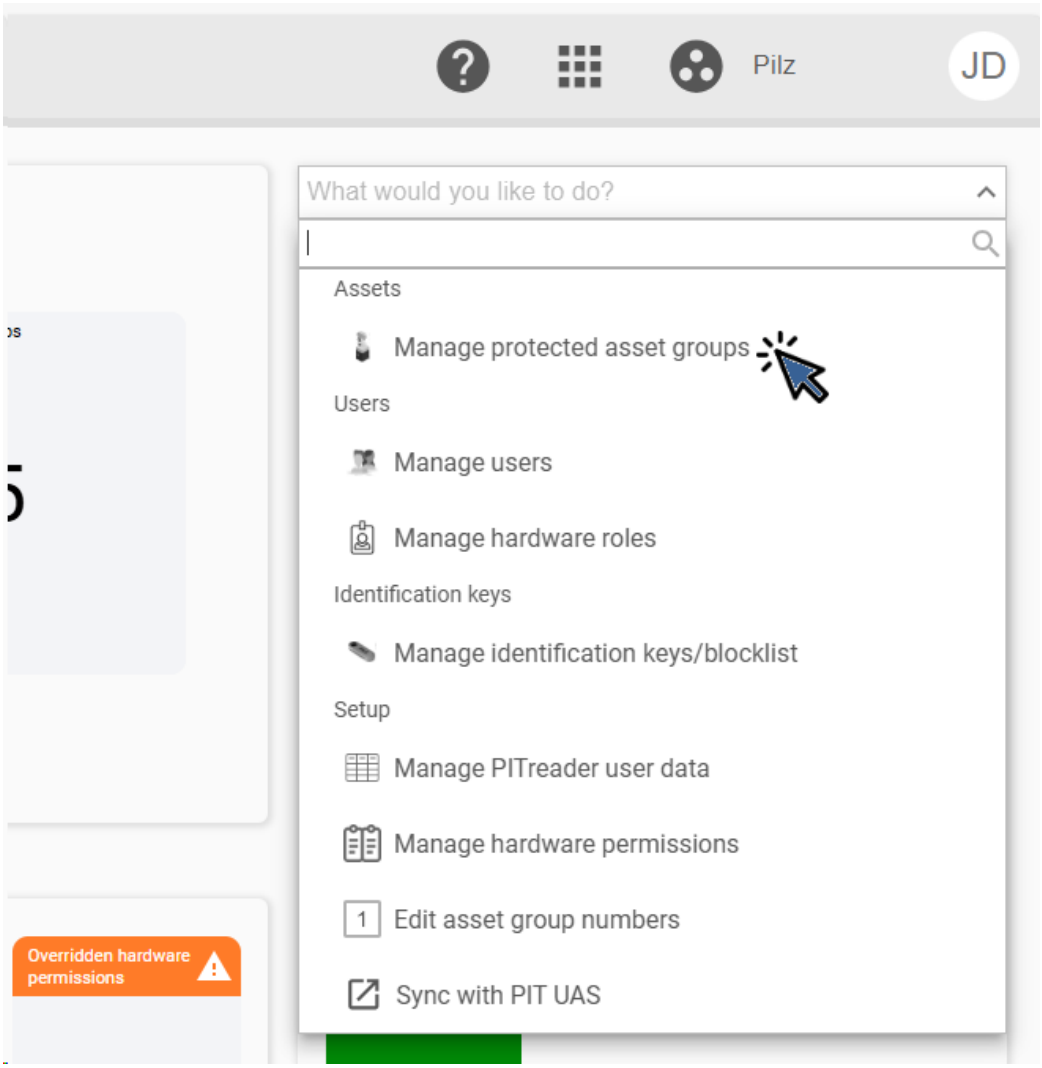


Method 2

The PITreader is added in the asset group.

1. Show asset groups

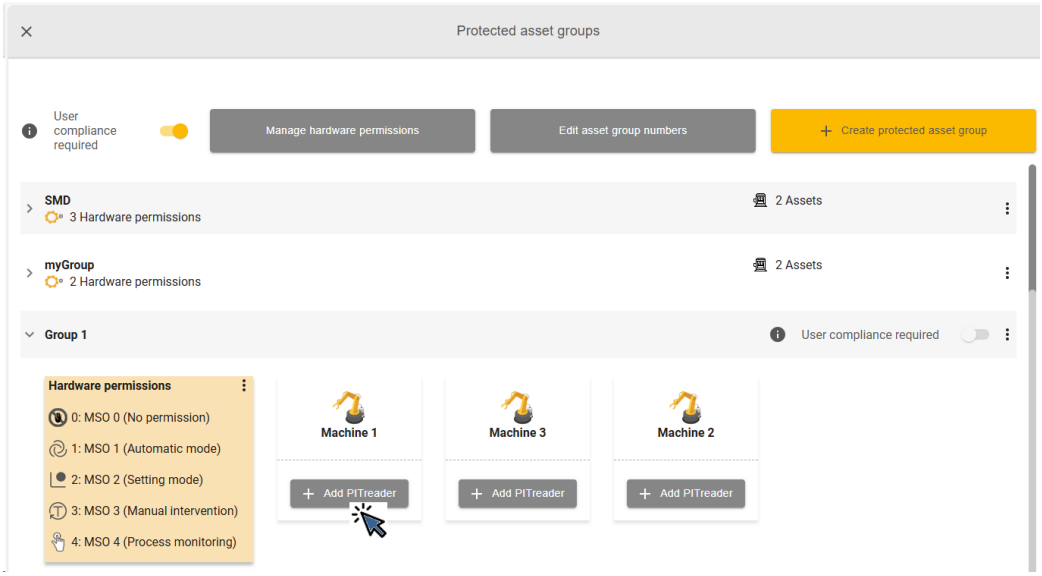
   ⇨ In the access management menu, select ***Manage protected asset groups***.



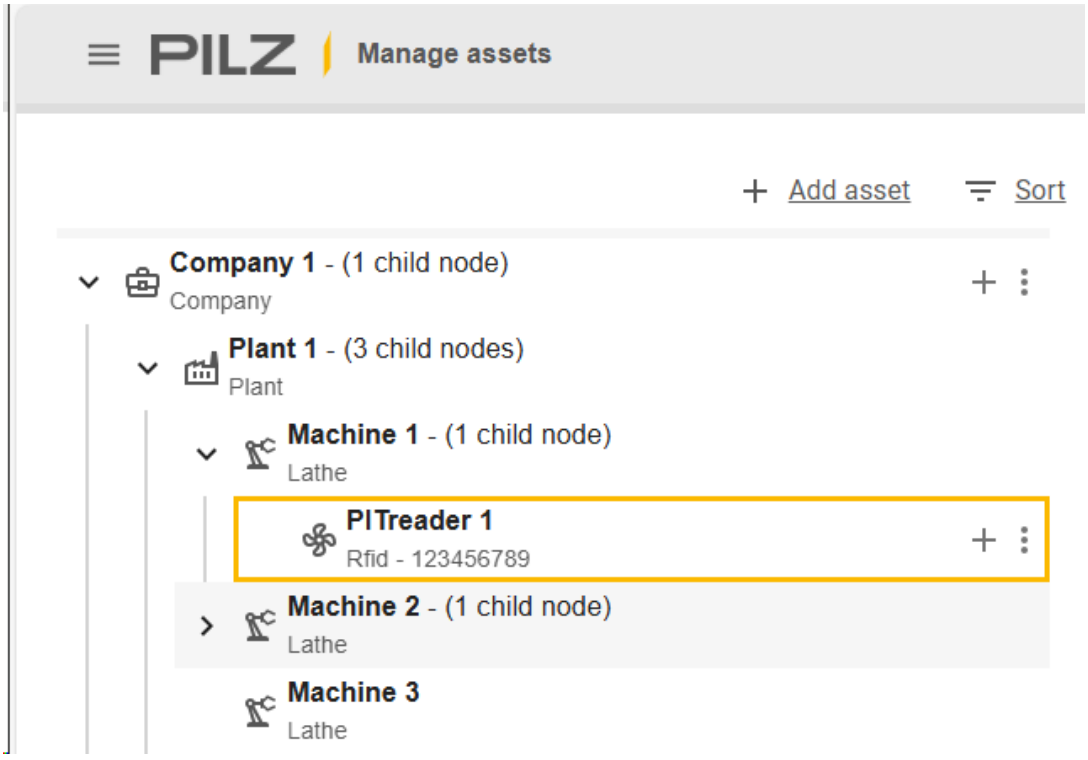
An overview of all the asset groups is displayed.

2. Add PITreader

   ⇨ Click on the asset group and then on ***Add PITreader***. Enter the necessary data and click on ***Save***.



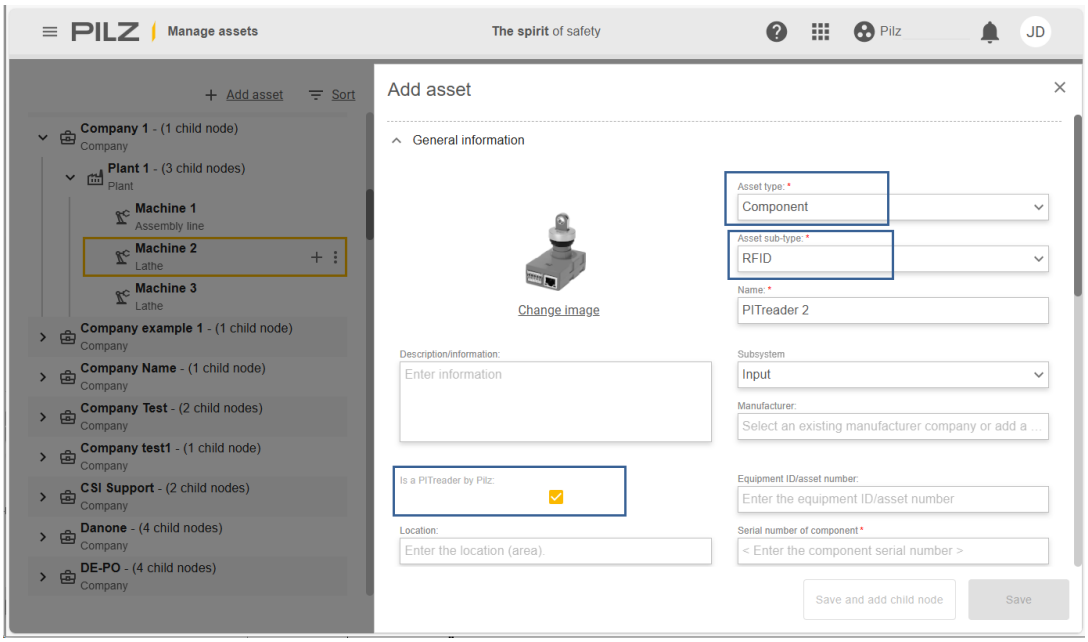
The PITreader can then also be found in asset management:



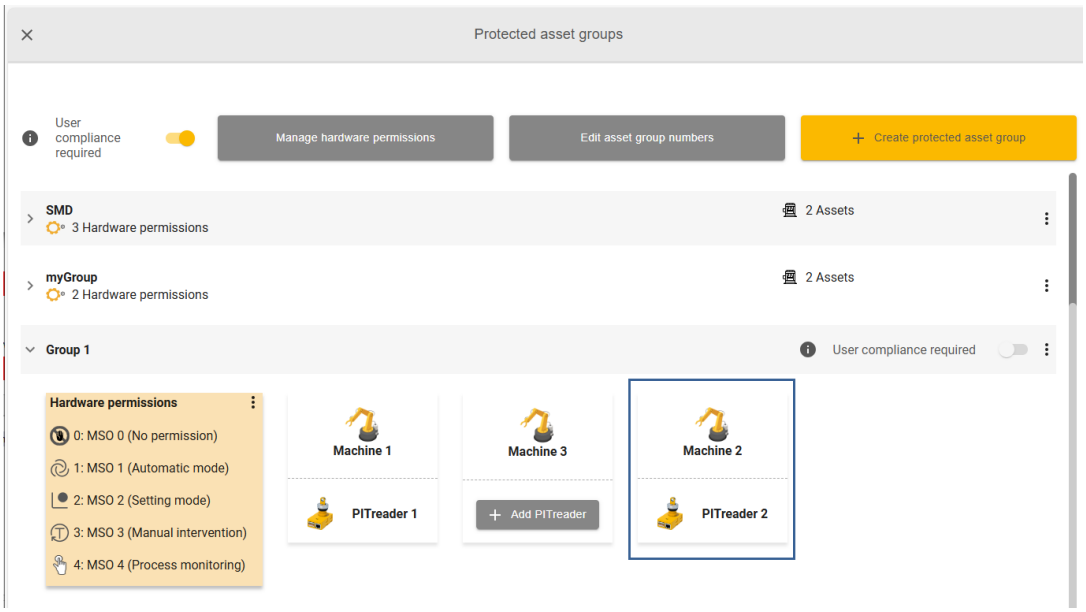
Method 3

In asset management, the PITreader is inserted under the machine as a component. There are a few settings to note here.

⇨ Open asset management and insert the PITreader under the machine. The 3 marked settings are important.



The PITreader is then assigned to the machine in the asset group:



6.4 Configure and use PITreader user data

Information about a user (e.g. language, user name, ...) can be stored in the PITreader user data; this information should be retrievable by the PIT UAS.
The user data is organised in parameters. For a user, the value of the parameter can be different for each asset group.

The values of the parameters can be defined individually for a user, or in the hardware role that is assigned to the user. But even if the user is assigned a hardware role, the values can still be adapted individually.

Prerequisites

- The action can be performed by users who have the following software role:
  – myAccessControl

Procedure

1. Open access management
   See Open access management [📖 33].
2. Start action
   ⇨ In the access management menu, select ***Manage PITreader user data***.
3. Create parameters
   ⇨ Click on ***Create parameters***.
4. Configure values for a user
   You have 2 options.
   Option 1: You configure the values of the parameters when you define the hardware permissions for the user.
   ⇨ On the access management dashboard, click on ***Protect user***. You can configure the values in one of the steps.
   Option 2:
   ⇨ In the access management menu, select ***Manage user***. In the row of the user, click on the ⋮ menu and select ***Edit user***.
   You can edit the values under ***Asset access***.

6.5 Assign hardware permission to users

On the MLP it is possible to determine the hardware permissions that apply to a user/ transponder.

First it is necessary to define what the hardware permissions should be. Only the names (numbers) of the hardware permissions are defined on the MLP. The practical significance of a hardware permission must be programmed in the safe evaluation unit (e.g. PIT m4SEU) or control system.
Then, for each asset group, it is necessary to define which of the created hardware permissions are used for the group.
These two actions can be performed when creating an asset group (see Create asset group [📖 34]).

Then, for each user, it is necessary to define the hardware permission they have for each individual asset group:

- Direct hardware permission
  Hardware permissions can be assigned to the user directly.
- Hardware role
  If there are several users who have the same tasks, it is also possible to create hardware roles. In the hardware role, a permission is defined for each asset group. The hardware role is then assigned to all users who have the same tasks. It is necessary at times to

grant a user temporary additional permissions to perform a task outside of their standard role. In this case, the permissions for this user can be changed for individual asset groups.

Prerequisites

- The action can be performed by users who have the following software role:
  - myAccessControl

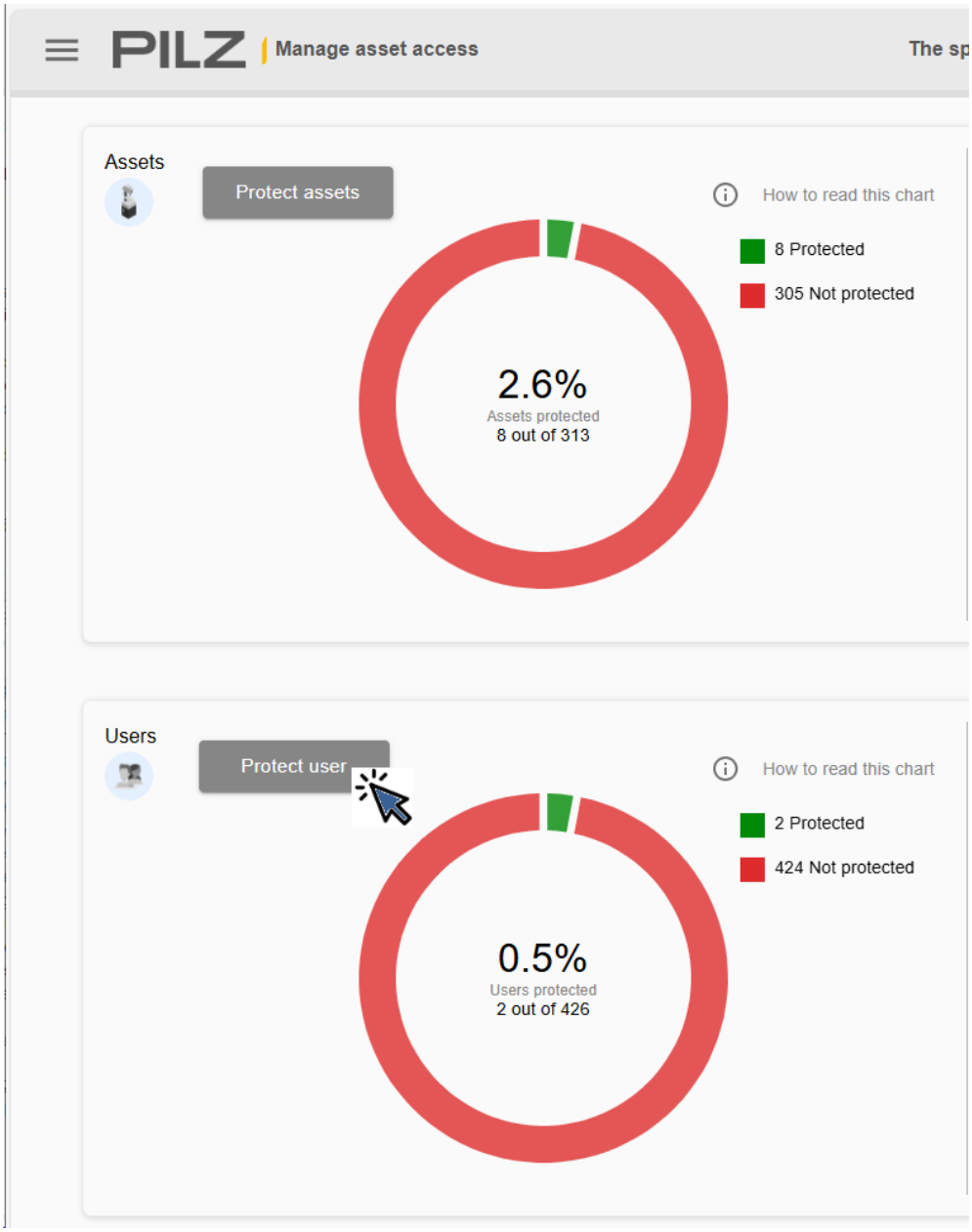
Procedure

1. Open access management

   See Open access management [📖 33].

2. Start action

   ⇨ Click on ***Protect user***.



3. Perform steps

   You will be guided through the steps required.

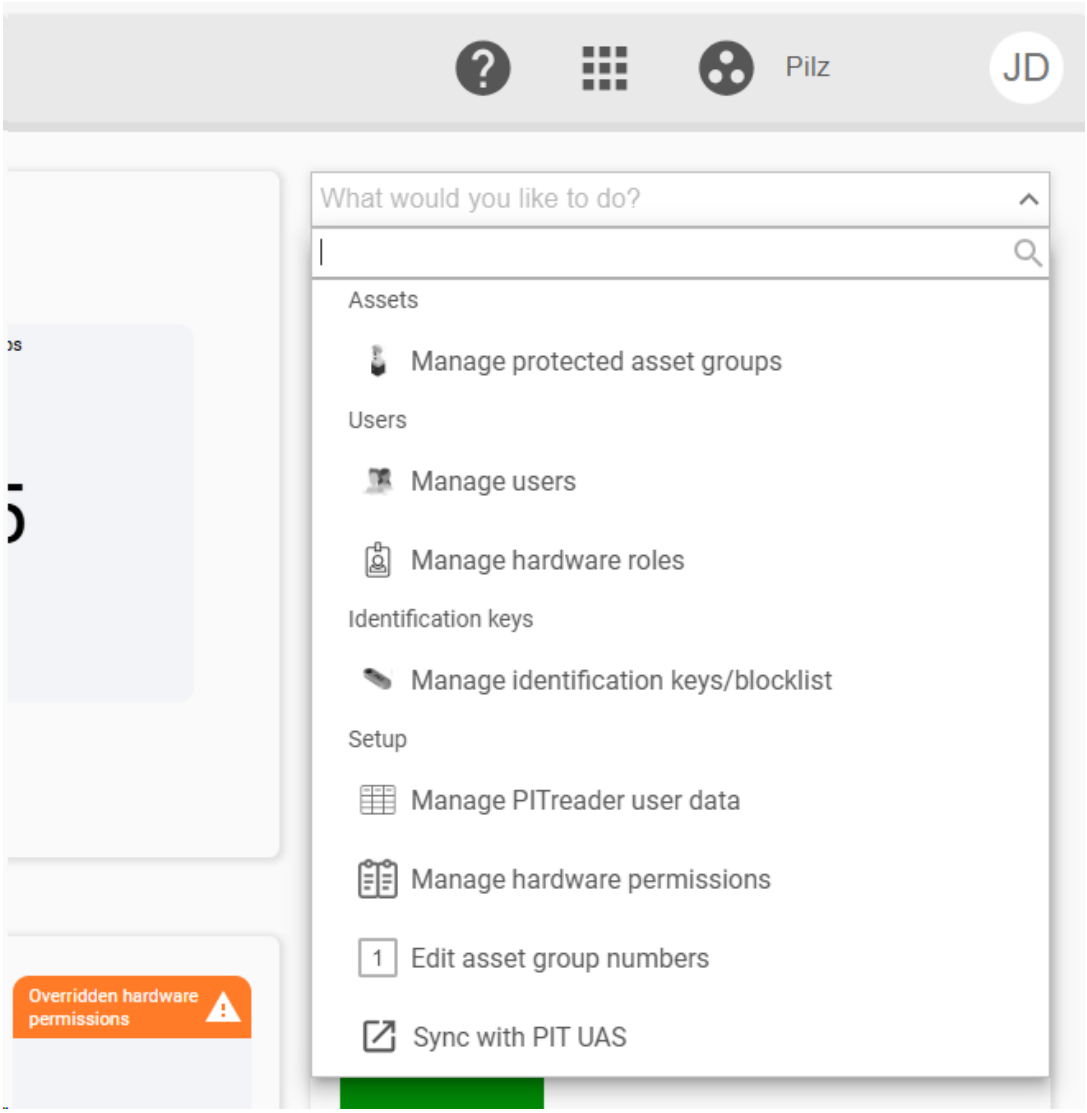
   ⇨ Follow the instructions.

4. Protect next user

   ⇨ Repeat step 2 for each user that you wish to protect.

Notes

If you wish to change individual settings, you'll find the actions in the central menu:



- Create, edit or delete hardware permissions
  - Select ***Manage hardware permissions*** from the menu.
- Create, edit or delete hardware roles
  - Select ***Manage hardware roles*** from the menu.
- Edit a user's hardware permissions
  - Select ***Manage users*** from the menu. In the row of the user, click on the ⋮ menu and select ***Edit***.

You can edit the hardware permissions under ***Asset access***.

- Edit or block identification keys
  - Select ***Manage identification keys/block list*** from the menu.

6.6 Assign identification key to users

Exactly one identification key must be assigned to each user. The user positions the identification key on the PITreader, so that authentication and authorisation can take place.

Prerequisites

- The action can be performed by users who have the following software role:
  - myAccessControl

Procedure

1. Open access management

   See Open access management [📖 33].

2. Assign identification key

   You have 2 options:

   Option 1: You assign the identification key when you define the hardware permissions for the user.

   ⇨ On the access management dashboard, click on ***Protect user***. You can assign the identification key in one of the steps.

   Option 2:

   ⇨ In the access management menu, select ***Manage identification keys/block list***. You can add a new identification key to the list and assign it to a user or you can edit an existing identification key.

6.7 Edit asset group numbers

Each asset group has a name on the MLP. The PITreader does not know these names, but works with numbers for the device groups.

You can define which number each asset group should have, i.e. which device group on the PITreader it corresponds to.

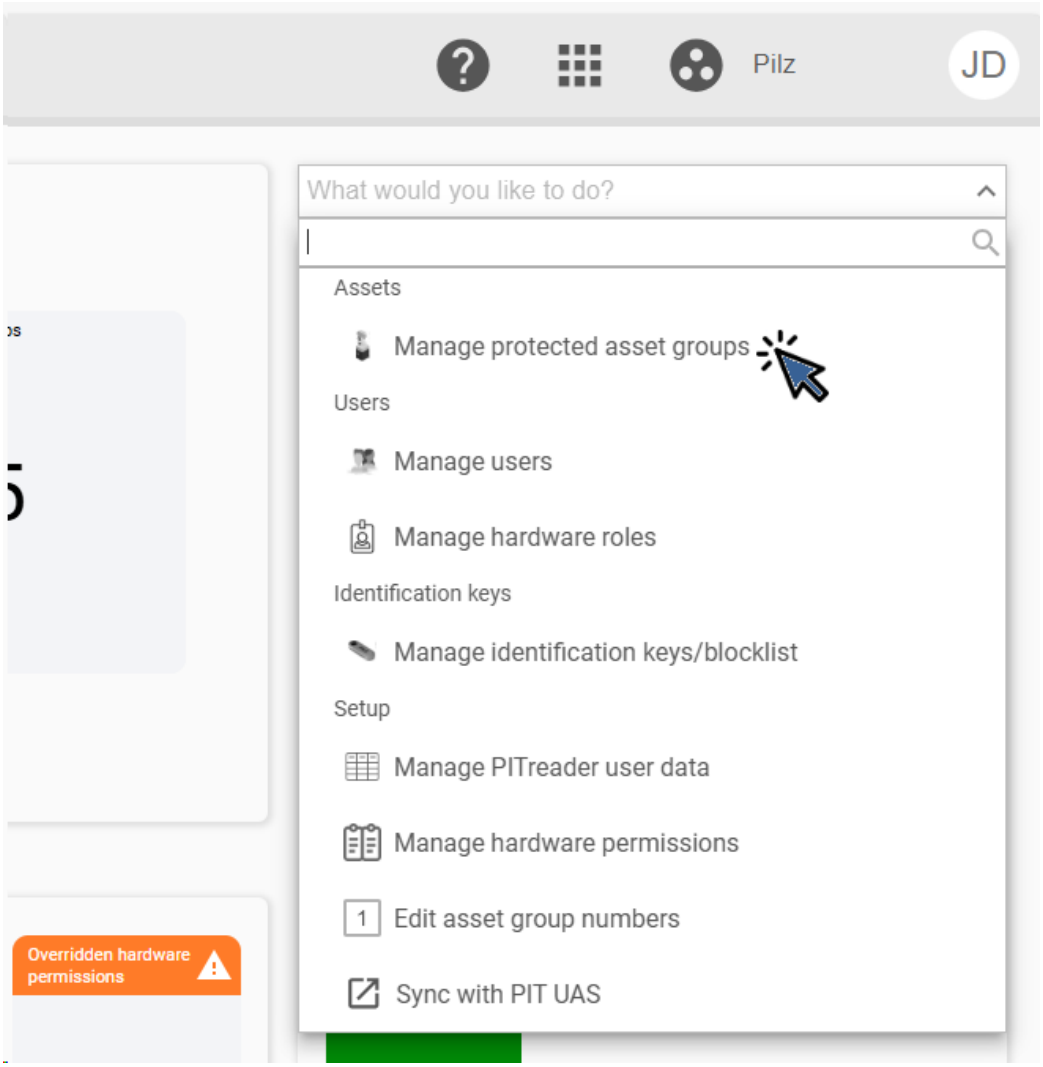
Prerequisites

- The action can be performed by users who have the following software role:
  - myAccessControl

Procedure

1. Show asset groups

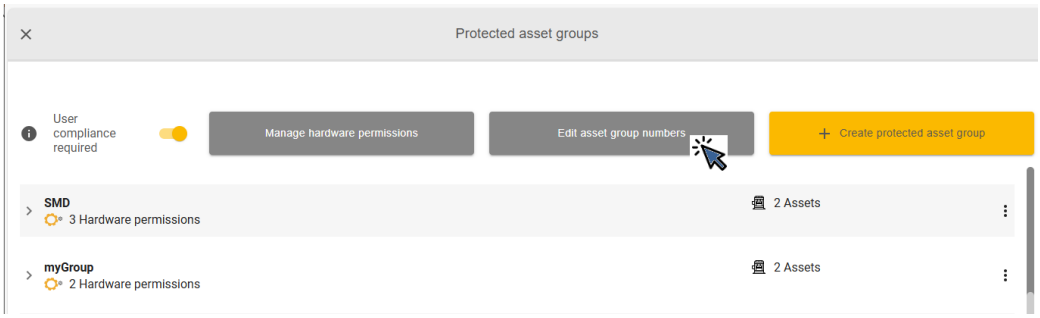
   ⇨ In the access management menu, select ***Manage protected asset groups***.



An overview of all the asset groups is displayed.

2. Start action

   ⇨ Click on ***Edit asset group numbers***.



3. Define numbers

   ⇨ Drag each asset group to the corresponding numbered box.

6.8 Define numbers for hardware permissions

The hardware permissions that are to be used for an asset group are defined. Each hardware permission has a name on the MLP. The PITreader does not know these names, but works with numbers for the permissions.

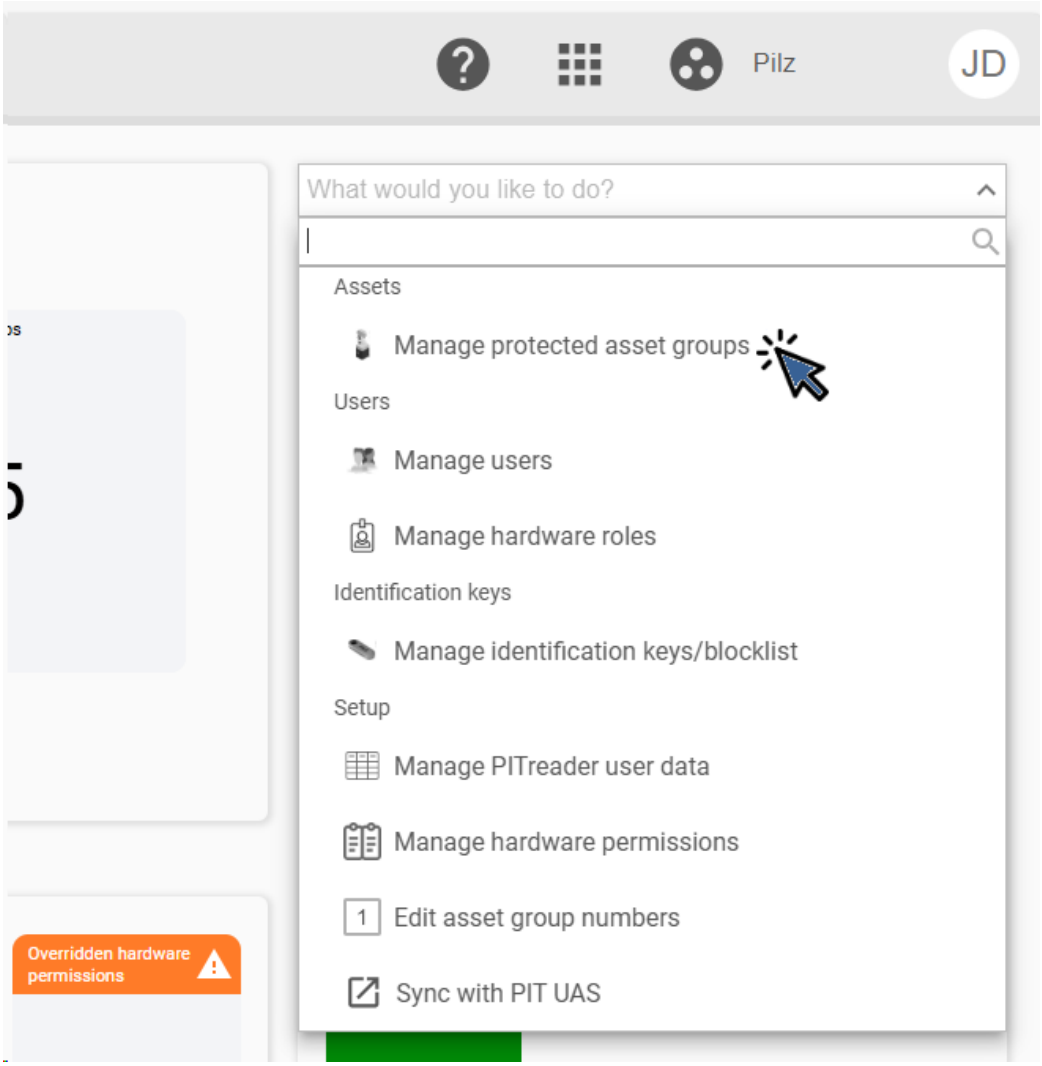
You can define the number of each hardware permission individually for each asset group.

Prerequisites

- The action can be performed by users who have the following software role:
  - myAccessControl

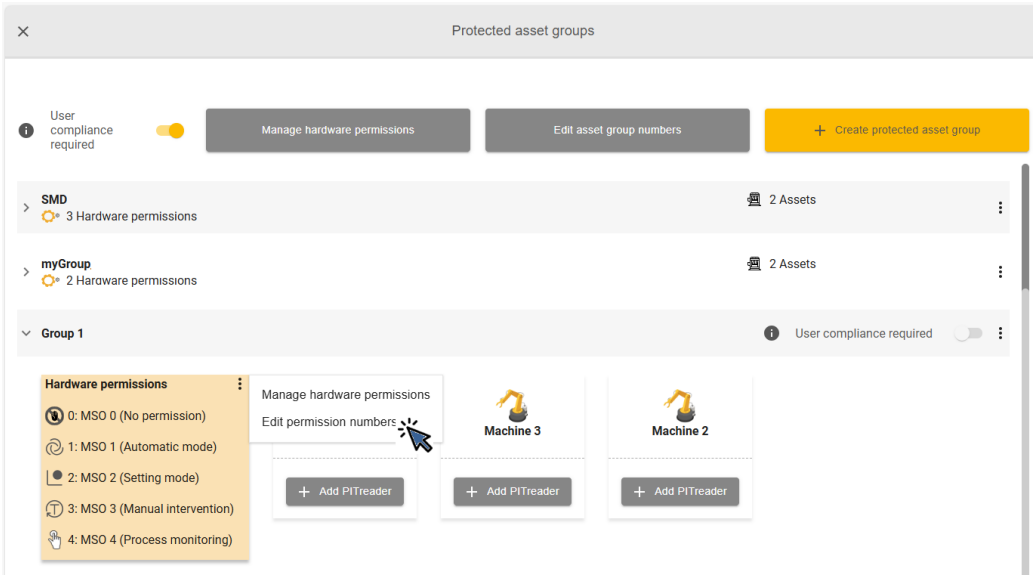
Procedure

1. Show asset groups
   ⇨ In the access management menu, select ***Manage protected asset groups***.



   An overview of all the asset groups is displayed.

2. Start action
   ⇨ Click on the asset group and select ***Edit permission numbers***.



3. Define numbers
   ⇨ Drag each permission to the corresponding numbered box.

6.9 Sync data with PIT UAS

The configuration for PIT UAS can be carried out on the MLP. Whenever the configuration has changed, the data must be transferred again from the MLP to the PIT UAS.

As there is no connection between the MLP and PIT UAS, the transfer must be carried out using a file.

Prerequisites

▸ The action can be performed by users who have the following software role:

– myAccessControl

Procedure

1. Open access management

   See Open access management [📖 33].

2. Start action
   In the access management menu, select ***Sync with PIT UAS***.

   A file is exported.

3. Import file into PIT UAS
   ⇨ Import the file into PIT UAS.

Support

Technical support is available from Pilz round the clock.

Americas
Brazil
+55 11 97569-2804
Canada
+1 888 315 7459
Mexico
+52 55 5572 1300
USA (toll-free)
+1 877-PILZUSA (745-9872)

Asia
China
+86 400-088-3566
Japan
+81 45 471-2281
South Korea
+82 31 778 3300

Australia and Oceania
Australia
+61 3 95600621
New Zealand
+64 9 6345350

Europe
Austria
+43 1 7986263-444
Belgium, Luxembourg
+32 9 3217570
France
+33 3 88104003
Germany
+49 711 3409-444
Ireland
+353 21 4804983
Italy, Malta
+39 0362 1826711
Scandinavia
+45 74436332
Spain
+34 938497433
Switzerland
+41 62 88979-32
The Netherlands
+31 347 320477
Türkiye
+90 216 5775552
United Kingdom
+44 1536 462203

You can reach our international hotline on:
+49 711 3409-222
support@pilz.com

Pilz develops environmentally-friendly products using ecological materials and energy-saving technologies. Offices and production facilities are ecologically designed, environmentally-aware and energy-saving. So Pilz offers sustainability, plus the security of using energy-efficient products and environmentally-friendly solutions.

BLUEcoMPETENCE Alliance Member
Partner of the Engineering Industry Sustainability Initiative

German Standards
BRAND OF THE CENTURY 2022

Quality Management ISO 9001:2015 REG. NO. 2462
Environmental Management ISO 14001 REG. NO. 2462
Energy Management ISO 50001 REG. NO. 2462

We are represented internationally. Please refer to our homepage www.pilz.com for further details or contact our headquarters.

Headquarters: Pilz GmbH & Co. KG, Felix-Wankel-Straße 2, 73760 Ostfildern, Germany
Telephone: +49 711 3409-0, E-Mail: info@pilz.com, Internet: www.pilz.com

PILZ
THE SPIRIT OF SAFETY

1006876-EN-02, 2025-04 Printed in Germany