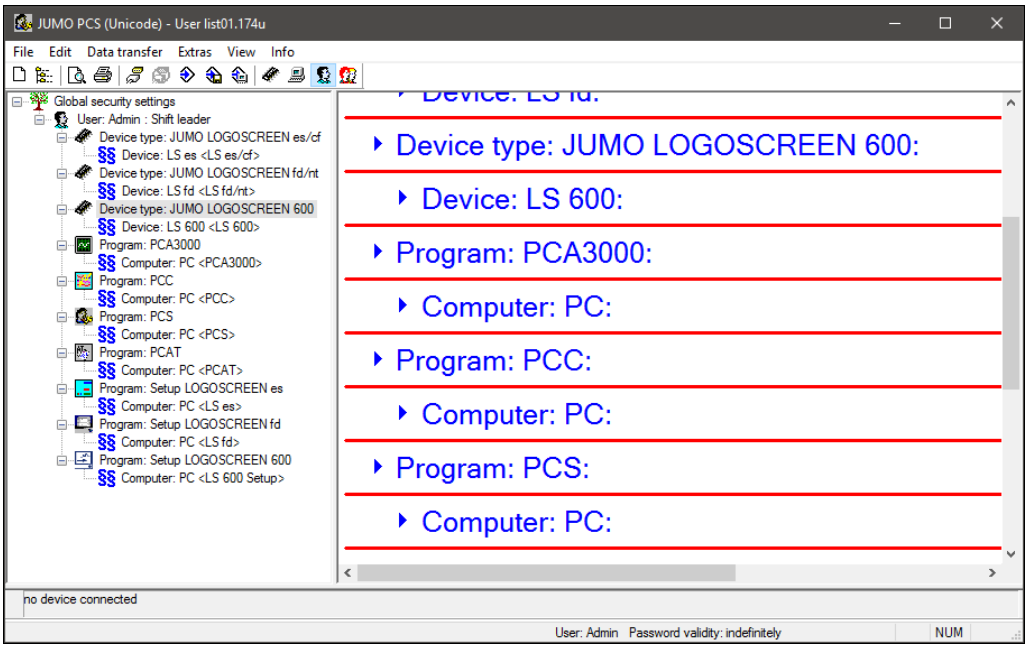
JUMO PC-Security-Manager-Software

PCS



Operating Manual

70970300T90Z001K000

V3.00/EN/00420782/2020-07-30

The present operating manual is valid for the software PC-Security-Manager-Software PCS as of version 174.03.xx.

Contents

Contents

Contents

1.1 Preface

Before installing and starting up, this manual must be read carefully.

The manual is an integral part of the product and must be stored for subsequent use.

If you would like further information or if problems occur that are not covered by the manual, the required information can be obtained from the manufacturer.

Modifications and repairs to the product may only be performed if expressly permitted by this manual.

Only by observing all of the safety instructions and all safety/warning symbols in these instructions can optimum protection of both personnel and the environment, as well as safe and fault-free operation of the device, be ensured.

1.2 Arrangement of the documentation

The documentation for this software is addressed to equipment manufacturers (OEMs) and users with appropriate technical expertise.

1.3 Typographical conventions

Warning symbols

Caution

This symbol is used when **damage to devices or data** may occur if the instructions are disregarded or not followed correctly!

Read documentation

This symbol, which is attached to the device, indicates that the device-specific documentation must be followed. This is necessary in order to recognize the nature of the potential danger and take the necessary measures to prevent it.

Note symbols

Note

This symbol is used to draw attention to a **particular issue**.

Reference

This symbol refers to **further information** in other manuals, chapters, or sections.

abc[1]

Footnote

Footnotes are remarks that **refer to** specific parts of the text. Footnotes consist of two parts:

An identification marking in the text and the footnote text.

The markers in the text are arranged as consecutive superscript numbers.

*

Action instruction

This symbol marks the description of a **required action**.

The individual work steps are indicated by asterisks, for example:

* Press ▲

* Confirm with ENTER

Display types

	Keys
▲ + ENTER	Keys are **shown in a box**. Keys can be expressed either as **symbols or text**. If a key has multiple functions, the text shown corresponds to the **function at the moment**.
	Menu items in the menu bar
FILE > **NEW**	Menu items appear in the document in a different font. Menu names, menu items, and submenu items (if applicable) are separated from one another by a ">".
	Menu items in the navigation tree and in the dialog window
"Export"	Menu items appear in the document in quotation marks.
	Symbol button
 Print	Buttons with a symbol appear in the document as an image.
	Text button
NEXT	Buttons with text appear in the document in a different font.
	Dialog windows and proper names
User log-in	Dialog window names or the proper name of a product appear in the document in bold.

1.4 Trademark information

- Microsoft® is a registered trademark of Microsoft Corp., Redmond, VA 98052-6399, US.
- Windows® is a registered trademark of Microsoft Corp., Redmond, VA 98052-6399, US.
- Windows Server® is a registered trademark of Microsoft Corp., Redmond, VA 98052-6399, US.
- CompactFlash® is a registered trademark of SanDisk LLC, Milpitas, CA 95035-7933, US.

1 Introduction

2.1 General information

The PC security manager software (PCS) ensures that only authorized persons have access to the system components (device, PC software) and sign electronic signatures in electronic documents.

External password specifications can also be implemented using the password rules.

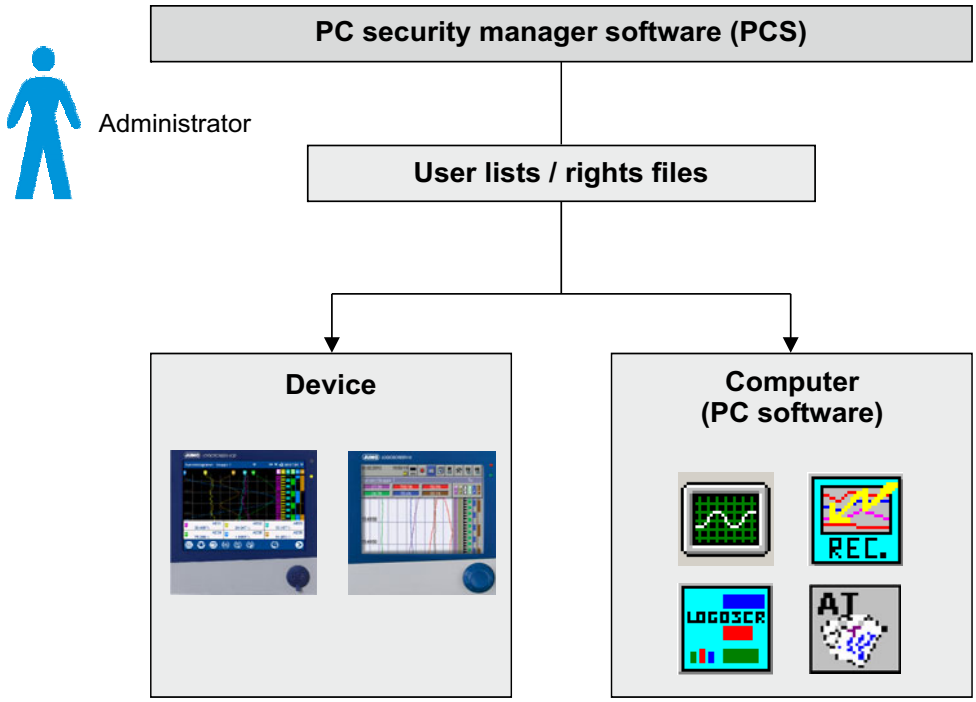
⇨ Chapter 5.1 "Password rules"

Only system administrators using an administrator PC are able to configure the security manager.

PC- and device-dependent user lists (rights files) are generated by the administrator and transferred to various PCs and/or devices.

User lists User lists are generated using the PCS software.

Rights files Rights files (for devices and computers) are formed from the user lists and sent to devices and/or computers.



Scope of delivery The PCS software is supplied on a data carrier or can be downloaded together with the following PC programs:

- Setup software
- PC Evaluation Software (PCA3000)
- PCA Communication Software (PCC)
- PC Audit Trail Software (PCAT)

2 The PC security manager software

2.2 Hardware and software requirements

Minimum configuration

The following hardware and software requirements must be met to operate and install the PCS:

- Notebook or desktop PC
- USB port, network connection or free serial interface (depending on the type of data transfer to the device)
- Windows 7 (SP1) or newer
- compatible Windows Server systems

2.3 "FDA 21 CFR Part 11"-compatible devices

The PC Security Manager software is available for the following devices:

Order code	Designation
706520	JUMO LOGOSCREEN 600
706521	JUMO LOGOSCREEN 601
706530	JUMO LOGOSCREEN 700
706560	JUMO LOGOSCREEN es
706585	JUMO LOGOSCREEN fd

The CD-ROM or download file for "FDA 21 CFR Part 11"-compatible devices also includes:

- Setup software
- PC Evaluation Software (PCA3000)
- PCA Communication Software (PCC)
- PC Audit Trail Software (PCAT)

The software for FDA inspections in "read-only mode" (PCA3000 Viewer) is freely available as a download for devices with increased safety standards.

Improper use, failure to observe this manual, the use of underqualified personnel, or unauthorized modifications releases the manufacturer from liability for any resulting damage. In these cases, the manufacturer's warranty no longer applies.

⇨ Prior to installation and startup, make sure that the operating staff are familiar with and understand the contents of the operating manual.

Prepare installation

* Connect a ready-to-use FDA-compliant device to a notebook or desktop PC via USB interface, network connection or a free serial interface and provide license numbers for FDA-compliant software.

Perform installation

* Select the features setup will install (at least **JUMO PCS**).

⇨ Chapter 4.1 "Starting installation"

* Enter appropriate license numbers for FDA-compliant software.
* Enter a local file path for the **user list** that also can be reached by network users.

⇨ Chapter 4.2 "Installation options"

* Complete the installation.

Starting the program

* Use the **User Lists Wizard** to create a new user list.

⇨ Chapter 5 "User lists wizard"

* The administrator can use the PCS to create a password for access to the PCS software for all users on the user list (devices and programs) and for himself.

⇨ Chapter 5.1 "Password rules"

* Define the Administrator and log on to the program.

⇨ Chapter 5.2 "Define administrator"

Application example

* In the **View according to users**, create the users who require device and program rights.

⇨ Chapter 7.4 "View according to users"

* Edit group with user rights in the respective **group pool** of the device or program.

⇨ Chapter 7.5 "View according to group pools"

* Assign device and program rights to the users.

⇨ Chapter 7.4.5 "New device/program rights"

* Transfer **user rights data** to the respective device.

⇨ Chapter 8.1.6 "Device rights file for the device"

3 Quick introduction

4.1 Starting installation

Installation from CD

* Start Microsoft Windows

If Microsoft Windows is already running, all Windows programs must be closed before installing the software.

* Insert the CD into the drive and close the drive.

The installation program starts automatically. If the installation program does not start:

* Start the "Setup.exe" file in the main directory of the CD.

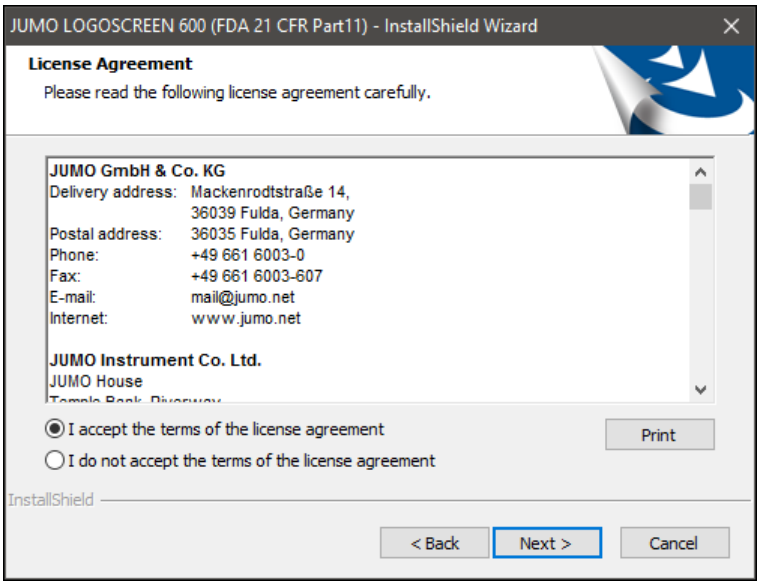
The installation program guides you through the rest of installation with on-screen prompts.

Installation via download file

After downloading the installation file, run it in Windows Explorer and follow the installation instructions.

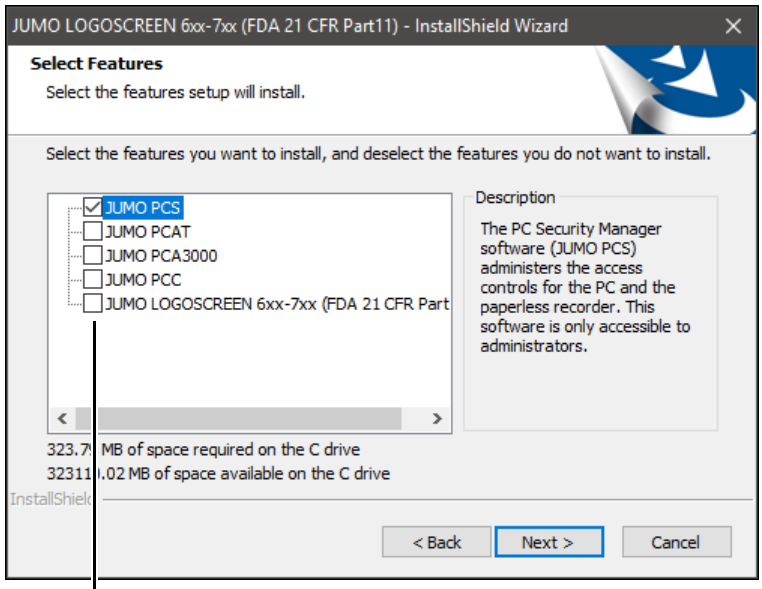
License agreement

* Read and confirm the license agreement.
  The agreement must be accepted before the software can be installed.



Available programs

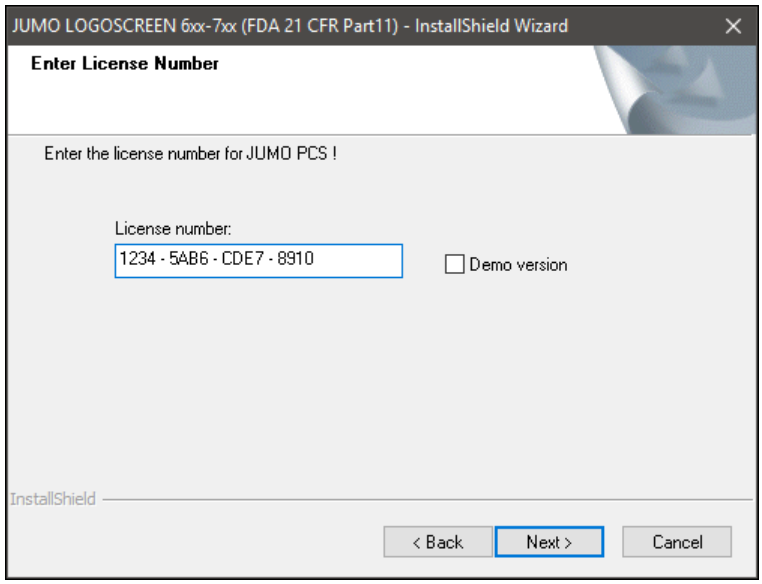
✱ Select the features (programs) you want to install.



The boxes of all components you want to install must be checked (☑).

PCS software is intended for use by administrators.

✱ Enter the license numbers for the selected programs.



If the "Demo version" option is enabled during the installation, some functions will be blocked in the selected software (e.g. data transfer, data storage and printing).
The software can be licensed at a later date. This will make all functions available.

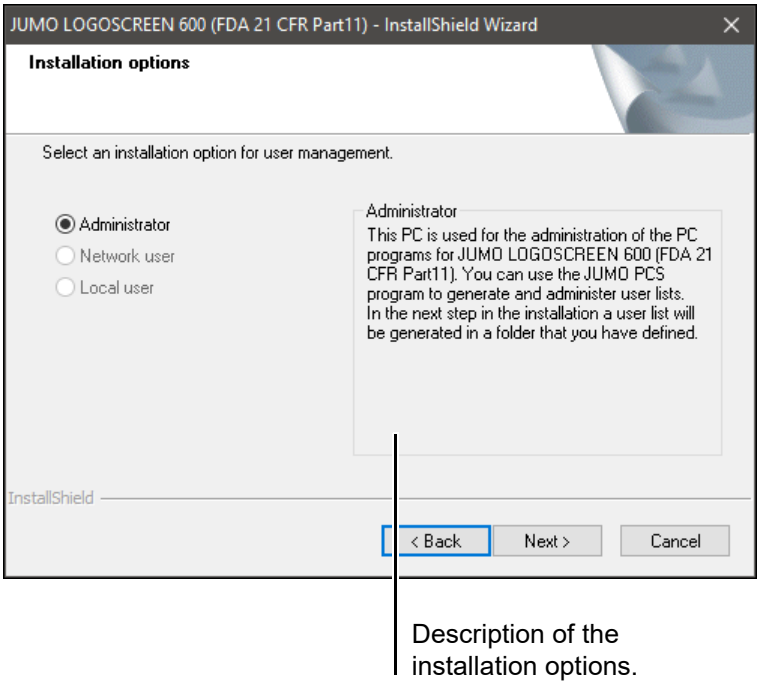
⇨ Chapter 10.4 "Extras"

Program folder

✱ Specify the program folder where the symbols for starting the software are to be copied.

4.2 Installation options

✱ Specify installation option



The installation options "Network user". page 18 and "Local user". page 18 require a user list or PC rights file to be generated beforehand.

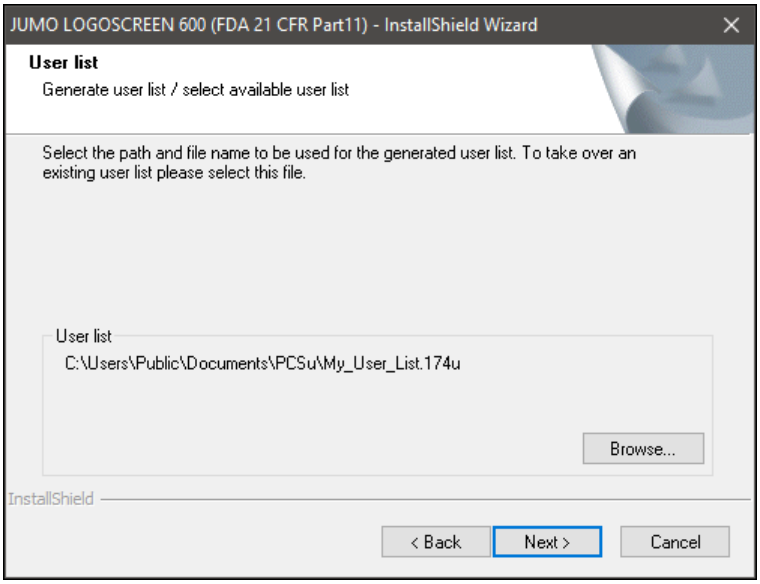
⇨ Chapter 9.2.2 "Generate PC rights file"

Administrator

The "Administrator" option is only available if the PCS software has been selected for installation.

The specified user list is regenerated with this installation option.

✱ Select the path and file name for the user list.



Network user

The "Network user" option is only available if the PCS software has **not** been selected for installation ("Available programs". page 16).

A user list is required for this installation option. This is only possible if, on a PC, an installation has been performed with the "Administrator" option, and a user list has been generated and stored on the network.

⇨ "Administrator". page 17

This user list is accessed each time the program starts.

Local user

The "Local user" option is only available if the PCS software has **not** been selected for installation ("Available programs". page 16).

A PC rights file is required for this installation option. This is only possible if, on a PC, an installation has been performed with the "Administrator" option, and a PC rights file has been generated and made available locally.

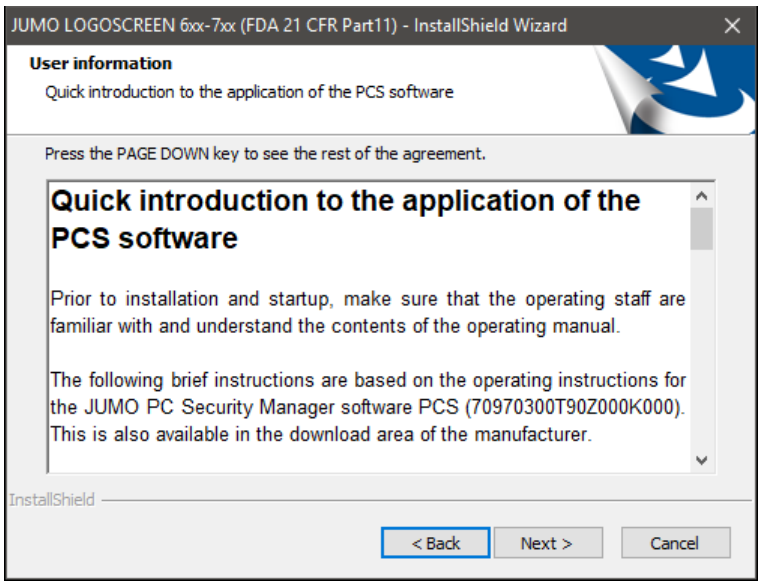
⇨ Chapter 9.2.2 "Generate PC rights file"

This list is no longer required after installation.

Perform installation

✱ Click the Install button

This is followed by a note with user information, which is also described in Chapter 3 "Quick introduction".



✱ Click the Next > button.

The selected software components are now installed.

✱ Allow JUMO PCS to start (☑) and terminate the installation by clicking the Finish button.

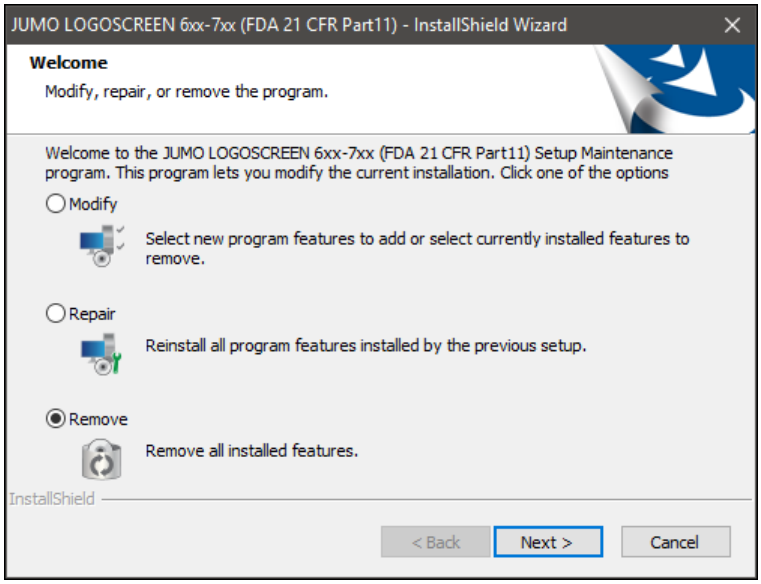
The PC security manager software now starts with the user lists wizard.

4.3 Uninstall PCS software

The user lists created using the PCS software are available under the paths and file names that already defined when the corresponding user lists were created.

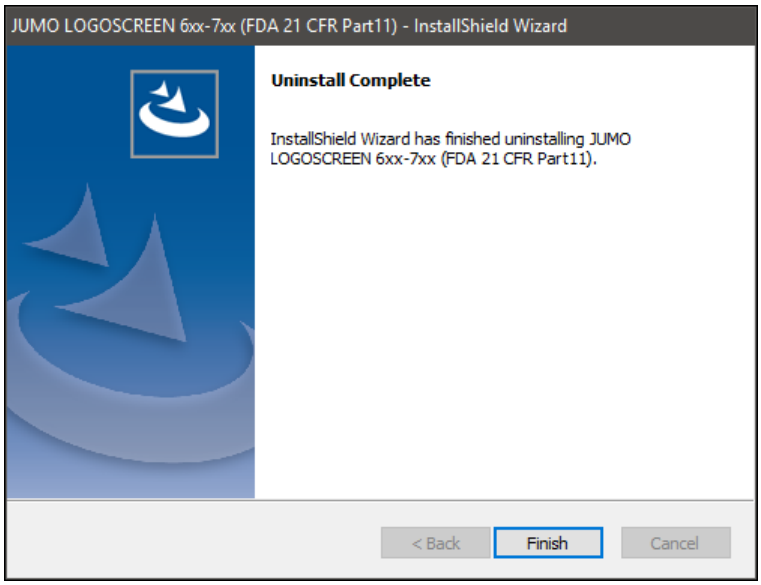
This data is not deleted by uninstalling the software.

* Start "Setup.exe" in the main directory of the CD or in the installation folder.



* Select "Remove" and confirm with Next >.

* Confirm uninstallation with Yes.

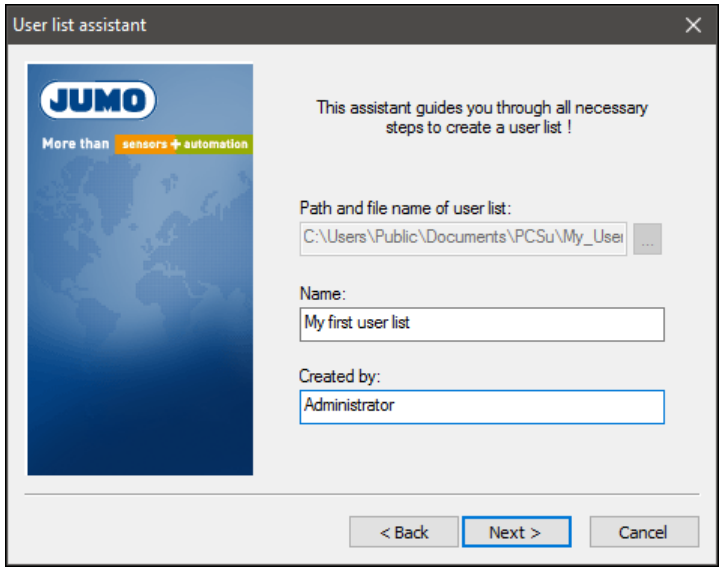


* Complete the uninstallation by clicking the Finish button.

The PCS software is completely uninstalled.

4 Installation

The user lists wizard starts up if the PCS software is reinstalled or if **FILE > NEW USER LIST** is used to generate a new user list. An entry mask appears where you can enter a designation for the user list and the author (administrator).



✱ Define "User list path and file name".

For reinstallation, the path and file name are already defined in a previous work step ("Administrator", page 17).

✱ Enter the "Designation" and "Author" of the user list in the entry fields.

The "Designation" and "Author" specifications are saved for the user list and can be changed at a later time. They are used for identification purposes in the following dialogs.

5 User lists wizard

5.1 Password rules

The administrator can use the PCS to create a password for access to the PCS software for all users on the user list (devices and programs) and for himself.

The structure of the password depends on the password rules.

Generate/change password rules	
Via the user lists wizard	⇨ Chapter 5.1.1 "Define password rules"
With an open user list	⇨ „Chapter 5.6 "Global security settings"
Generate/change password	
Via the user lists wizard	⇨ "Generate password", page 26
Via program logon	⇨ "Generate/change password", page 28
With an open user list	⇨ "Generate/change password", page 28 ⇨ Chapter 5.6 "Global security settings"

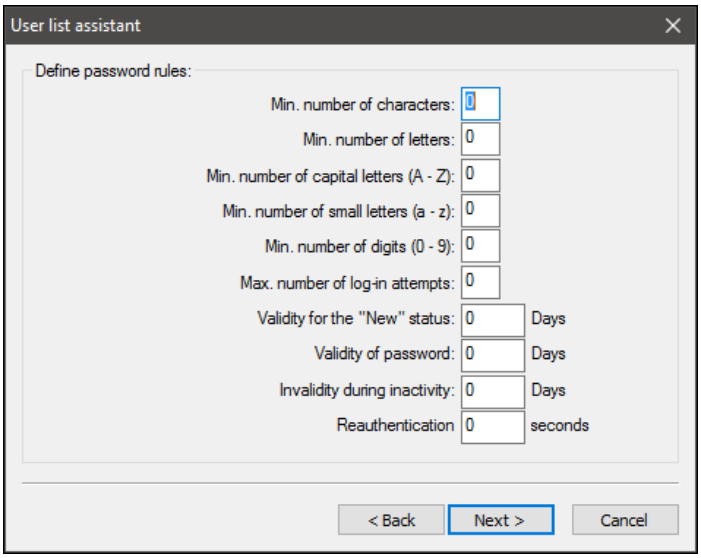
5.1.1 Define password rules

Specifying of password validities:

An access to the PCS software and the corresponding user list that has been blocked due to an expired period of inactivity can only be unlocked by the administrator using the reactivation code.

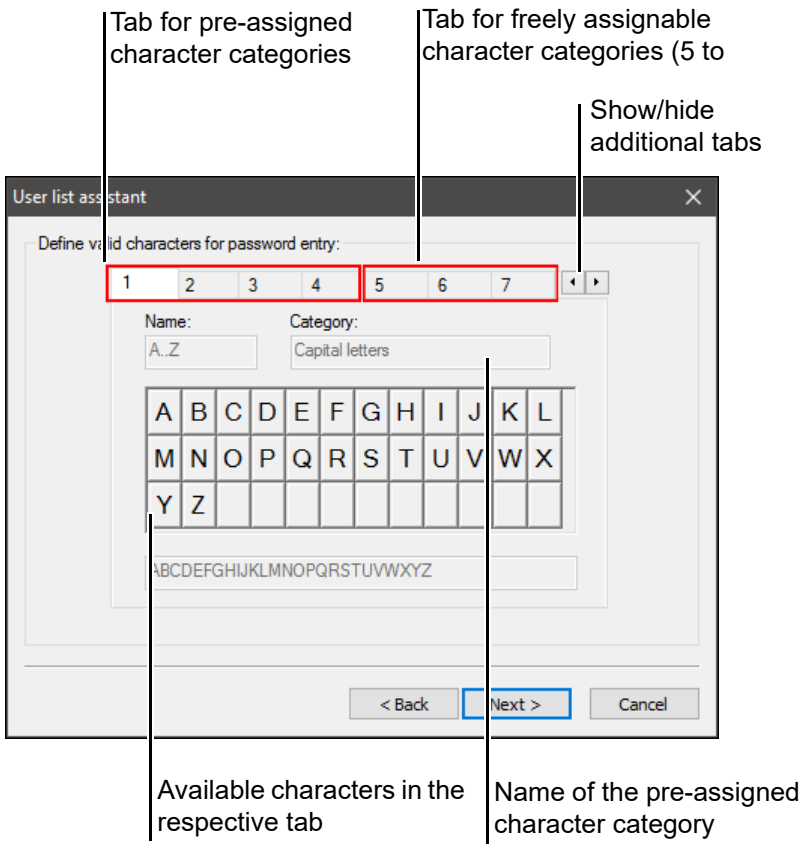
⇨ Chapter 5.5 "Reactivation code"

The password rules are defined using the following dialog:



Min. number of characters	Minimum number of characters (letters and numbers) that the password must have. 0 = any (between 1 … 10 characters can be entered).
Min. number of letters	Number of letters that the password must contain. 0 = No letters required.
Min. number of uppercase letters (A…Z)	Number of uppercase letters that the password must contain. 0 = No uppercase letters required.
Min. number of lowercase letters (A…Z)	Number of lowercase letters that the password must contain. 0 = No lowercase letters required.
Min. number of numbers (0...9)	Number of numbers that the password must contain. 0 = No numbers required.
Max. number of logon attempts	Number of failed logon attempts permitted for a user. 0 = No restriction. If not equal to 0, the number of invalid logon attempts is counted. If the number is exceeded, the user is blocked. Only the administrator can approve the user again. Each successful logon sets the counter back to 0.
Validity for the status "New"	When logging on to a device or piece of software for the first time, each user must change the password assigned to them. If the parameter is not equal to 0 days, the time between the creation of the user in the user list and the first log-on is checked. If the time exceeds the time specified here, the user is blocked. Only the administrator can lift a block. 0 = No check for "New" status.
Validity of the password	The password must be changed every x days. 0 = No change of password required.
Validity during inactivity	The user is blocked if he/she has not logged in again within the specified period of time after logging off. Only the administrator can lift a block. The "Validity during inactivity" setting is similar to the "Validity for New status" setting. The time between the last logon and the next logon is checked. 0 = No inactivity check.
Re-authentication	If no operational action is taken during the specified period of time (no buttons are pressed), the logged on user is automatically logged off. The user then needs to log on again before taking the next operational action. 0 = No re-authentication

5.1.2 Valid character for the password entry



Password characters

If a new user list is generated, 16 tabs are available. Tabs 1 to 4 are pre-assigned with password characters and cannot be changed. They are also divided into categories that can be selected when defining the password rules:

Tab	Category	Password rule
1	Uppercase letters	Min. number of uppercase letters
2	Lowercase letters	Min. number of lowercase letters
3	Numbers	Min. number of numbers
4	None	Min. number of characters

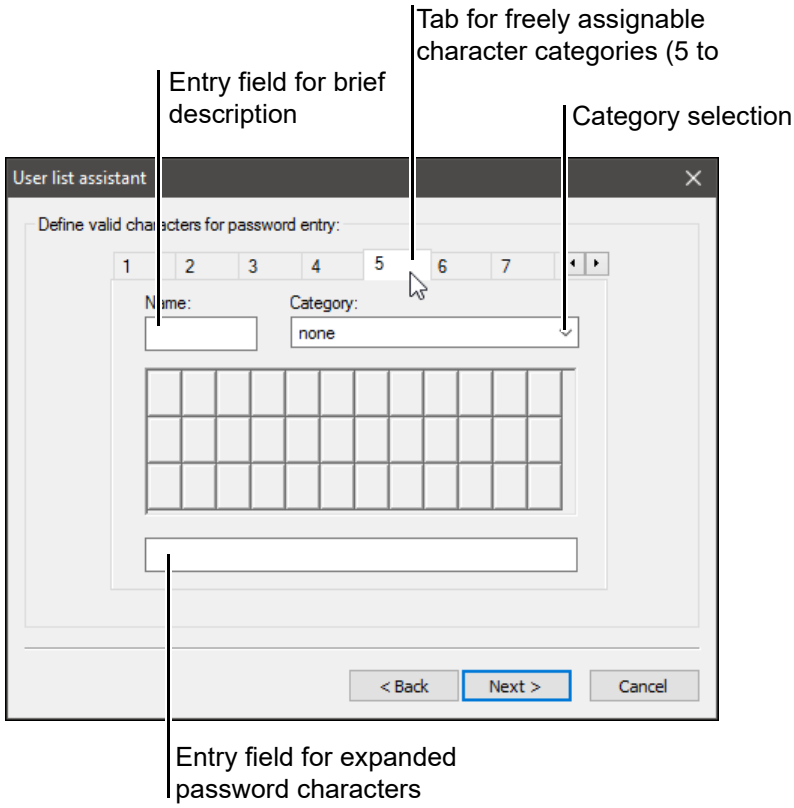
When a password is assigned for the first time, the default password characters available from tabs 1 to 4 can be used.

The author (administrator) can freely assign password characters for tabs 5 to 16.

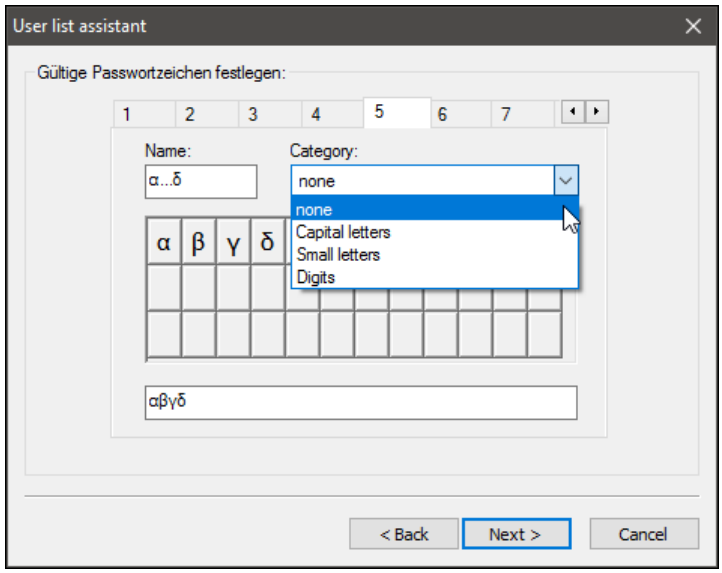
⇨ "Expand password characters", page 25

Expand password characters

Proceed as follows:



* Select tab for freely assignable character categories (tabs 5 to 16)
* Enter desired password characters in the entry field for expanded password characters.
* Enter a brief description in the "Name" entry field



* Select a suitable category for the new password characters.

⇨ Chapter 5.1 "Password rules"

5.2 Define administrator

* Enter the user ID and the name of the administrator. The "Description" entry field can be filled in as a supplement.

A user ID designation that has been used once cannot be edited; a user cannot be deleted.

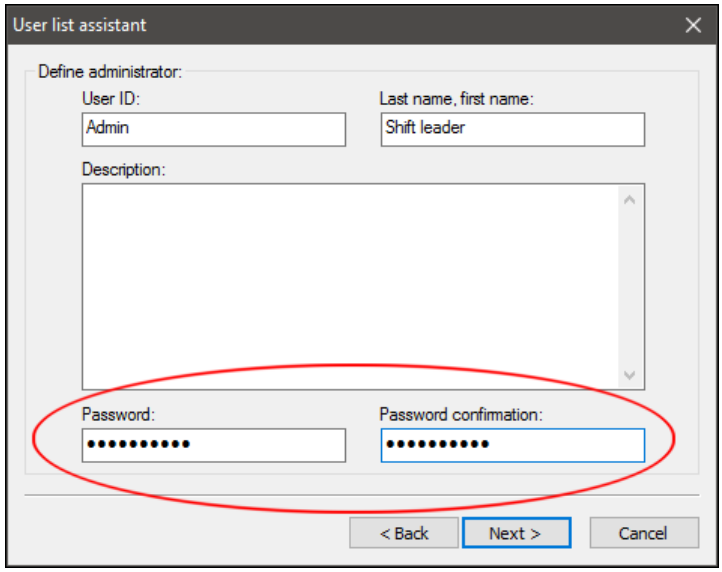
Generate password

If no corresponding password rules are defined in advance and no password characters have been expanded, a password can be generated here that consists of a maximum of ten (10) characters from the pre-assigned character categories.

The password fields only need to be filled in if the corresponding password rules were defined in advance.

If the intention is to generate the password in one of the following dialogs, it is a good idea not to define any password rules or fill in the password fields in advance.

⇨ "Generate/change password", page 28



* Then press the Next > and Finish buttons to close the user lists wizard.

If a user list is generated via **FILE > NEW USER LIST**:

The previous user list is now closed. All PC programs will work with the new user list from now on.

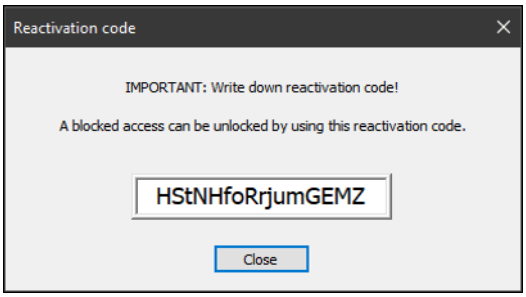
The **Reactivation Code** dialog window opens.

Reactivation code

Administrator: Always write down and keep the current reactivation code of a user list!

An access to the PCS software and the corresponding user list that has been blocked due to an expired period of inactivity can only be unlocked by the administrator using the reactivation code.

⇨ Chapter 5.5 "Reactivation code"

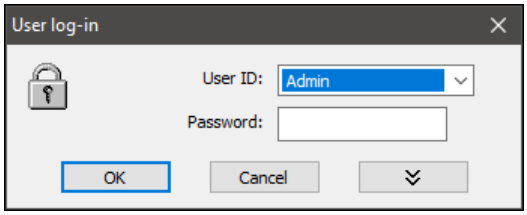


✱ Write down the reactivation code, keep it and finish with Close.

The program log-in follows.

5.3 Program log-in

Enter password



✱ Log on to the program using the name and password defined in Chapter 5.2. If no password was generated in Chapter 5.2, this entry field can remain blank.

✱ Confirm with OK.

If a password is to be created or changed subsequently:

⇨ Chapter 5.4 "Options for program start"

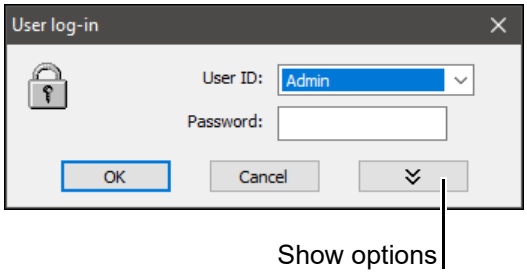
5 User lists wizard

5.4 Options for program start

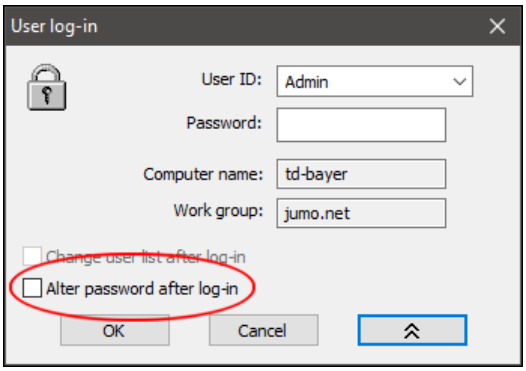
Generate/ change password

If the intention is to generate or change a password in this step, proceed as follows:

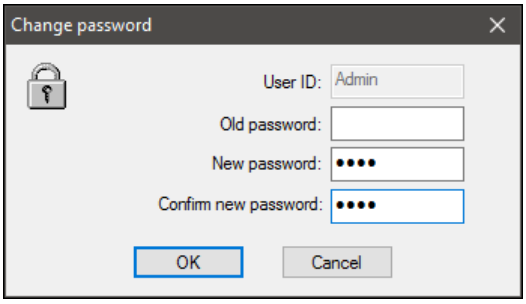
* Start the software.
* Left-click the » button before logging on



The dialog window changes to ...



* Tick the checkbox (☑) "Change password after logon".
* Press the OK button.
* The dialog window changes to ...



* Enter the previous (old) password. If no password was generated in Chapter 5.2, this entry field can remain blank.
* Enter the new password and confirm the password.
* Press the OK button.

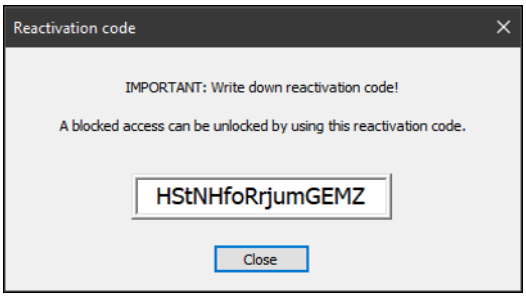
The **Reactivation Code** dialog window opens.

Reactivation code

Administrator: Always write down and keep the current reactivation code of a user list!

An access to the PCS software and the corresponding user list that has been blocked due to an expired period of inactivity can only be unlocked by the administrator using the reactivation code.

⇨ Chapter 5.5 "Reactivation code"



✱ Write down the reactivation code, keep it and finish with Close.

The user is now logged on under his/her ID (e.g. "Admin") and with his/her new password.

The user list has been created and can now be edited by the administrator.

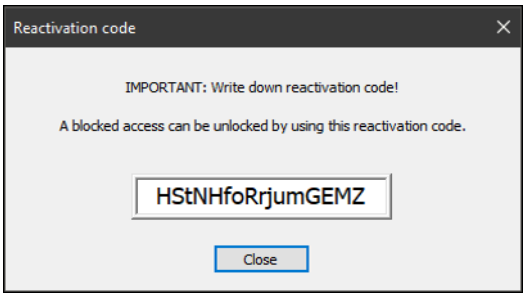
⇨ Chapter 7 "Edit user lists"

5.5 Reactivation code

When creating a user list, a user list-specific reactivation code is generated.

It is used by the administrator to unlock access to the PCS software and the corresponding user list that has been blocked by expired inactivity periods.

A reactivation code is always renewed when the administrator creates or changes the password of a corresponding user list.

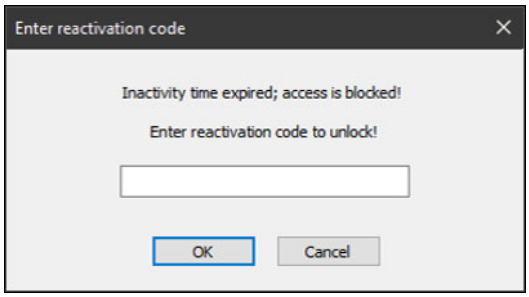


A reactivation code is user list-specific!

Administrator: Always write down and keep the current reactivation code of a user list!

Enter reactivation code

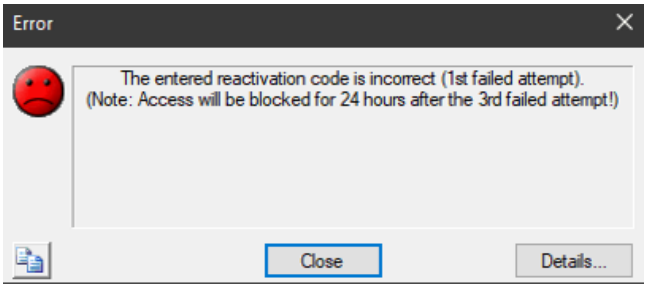
If access to the PCS software is blocked due to an elapsed period of inactivity, the following dialog window appears:



* Enter the current reactivation code.
* Confirm with OK.

Incorrect entry/ Loss of reactivation code

If an incorrect reactivation code is entered, the following dialog window appears:



Acces will be blocked for 24 hours after the 3rd failed attempt.

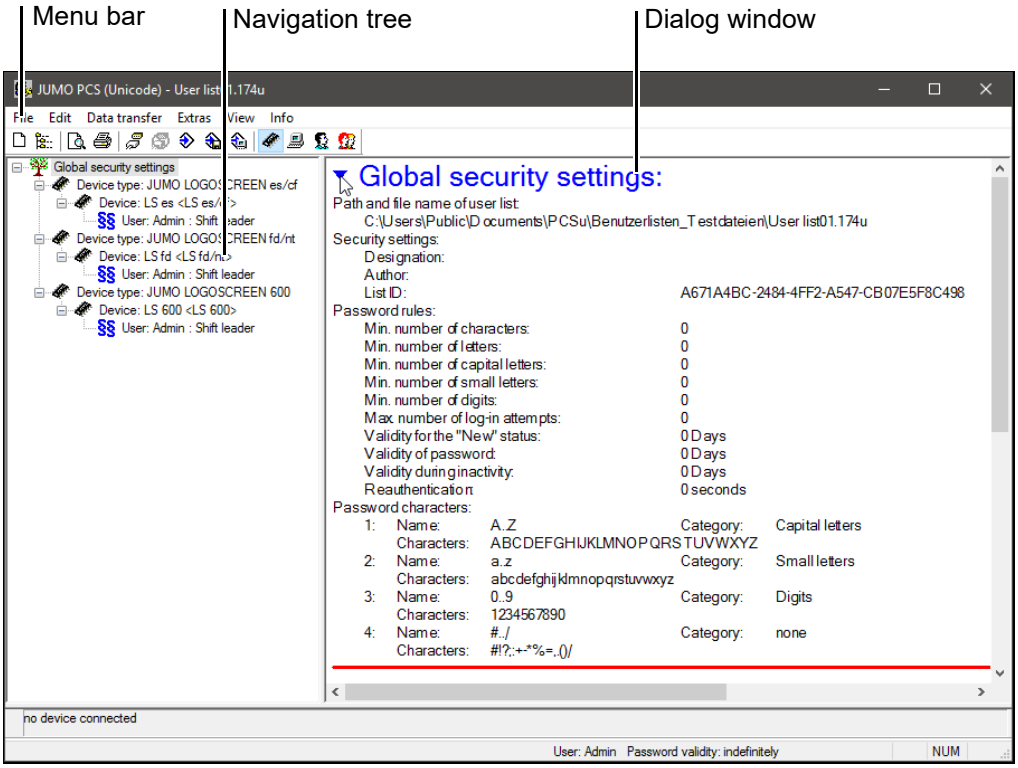
If the reactivation code is lost, the PCS software must first be uninstalled and then reinstalled.

⇨ Chapter 4.3 "Uninstall PCS software"

5.6 Global security settings

The parameters created by the user lists wizard are stored in the "Global security settings" entry after starting the program and when the user list is open.

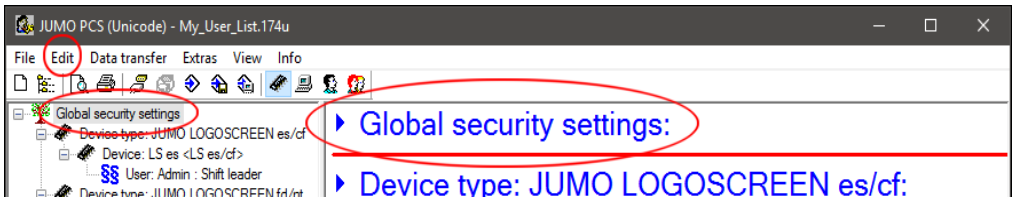
✱ Left-click the "Arrow pointing downward" (▼):



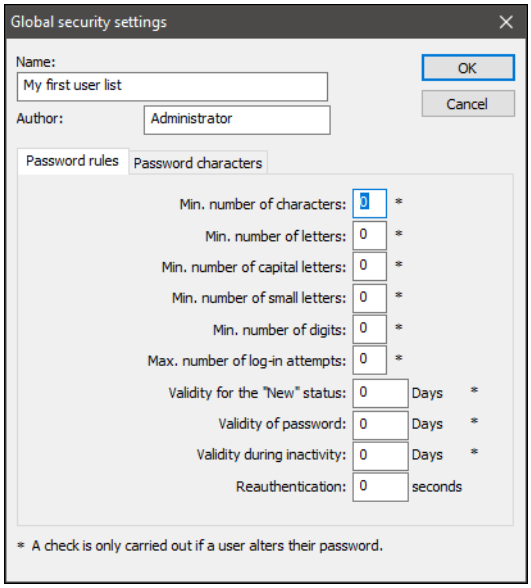
5.6.1 Edit global security settings

✱ Select the "Global security settings" navigation tree and right-click to open the "Global security settings" command

Alternatively, double-left-click on "Global security settings" in the dialog window or invoke the **EDIT > EDIT GLOBAL SECURITY SETTINGS** command via the menu bar.



The **Global security settings** dialog window opens. The settings can be edited.



Description ⇨ "User lists wizard", page 21

Author ⇨ "User lists wizard", page 21

Password rules ⇨ "Define password rules", page 22

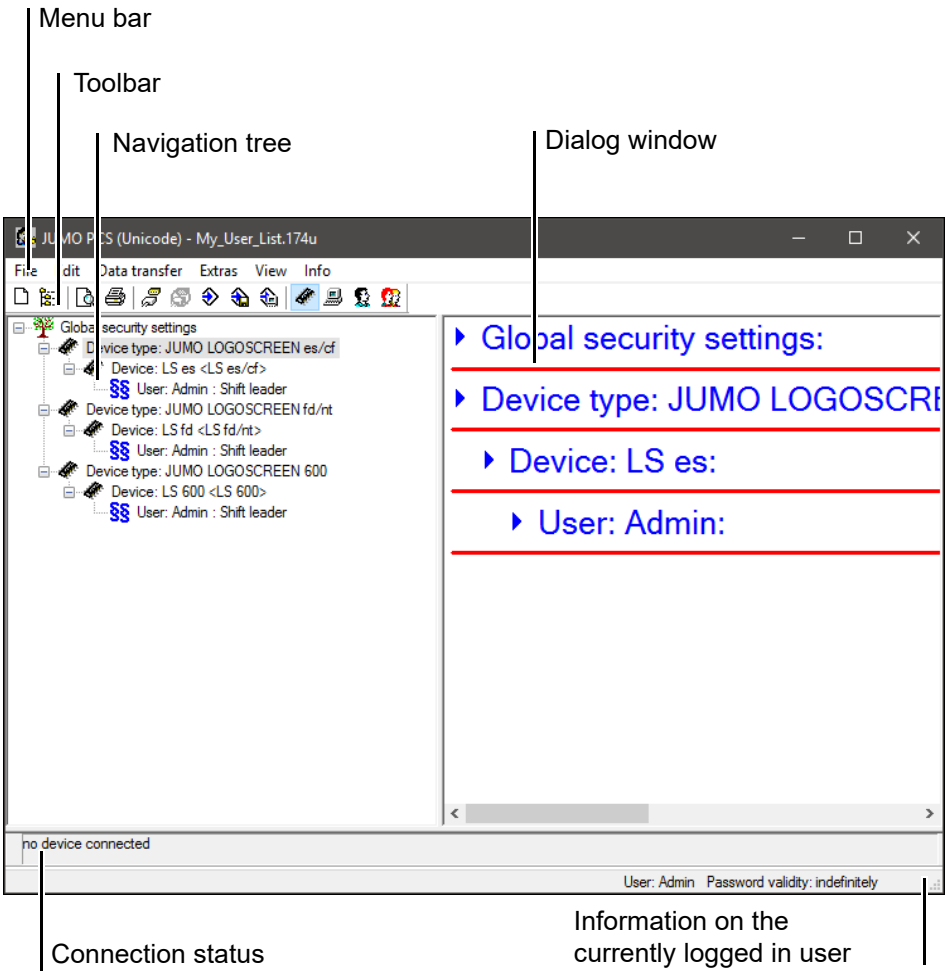
Password characters ⇨ "Valid character for the password entry", page 24

Changes can only be made to the password rules and the password characters if a user changes his/her password.

⇨ "Options for program start", page 28

⇨ "Renew logon/change password", page 121

6.1 Elements of the user interface



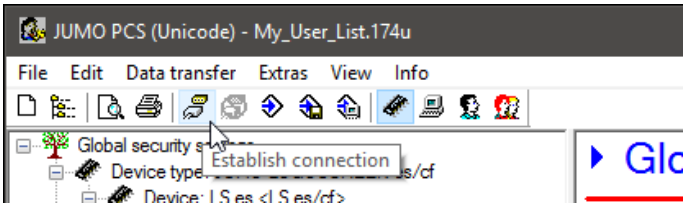
Menu bar

The menu bar can be used to launch the individual functions in the software.

⇨ Chapter 10 "Menu functions & symbols"

Toolbar

The toolbar contains selected functions from the menu bar. Left-click to start these functions. The name of the function will appear (pop-up text) when you briefly hover the mouse over one of the symbols.



⇨ Chapter 10 "Menu functions & symbols"

Work pane

The current settings are displayed in the work pane (navigation tree and dialog window). New entries and changes can be made here.

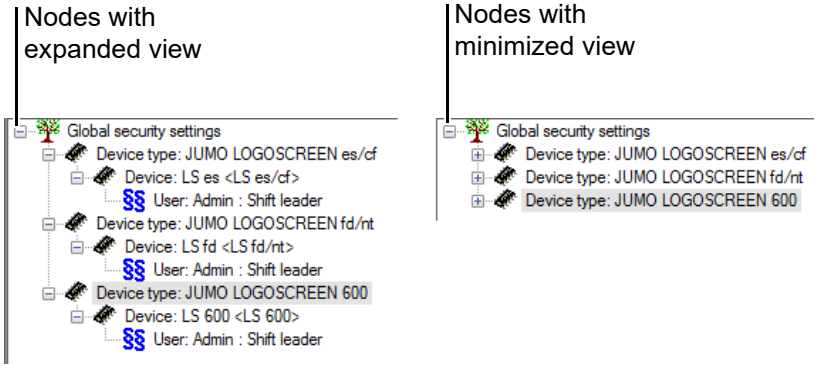
6.1.1 Navigation tree

Control dialog window

Left-clicking an entry in the navigation tree makes it appear in the dialog window.

Expand/collapse node

Left-clicking ⊟ collapses the node information, clicking ⊞ expands it again.



Alternatively, access the context menu by right-clicking an entry in the navigation tree and access the **Expand/collapse node** functions.

6.1.2 Dialog window

Start change dialog

Double clicking an entry in the dialog window starts the change dialog.

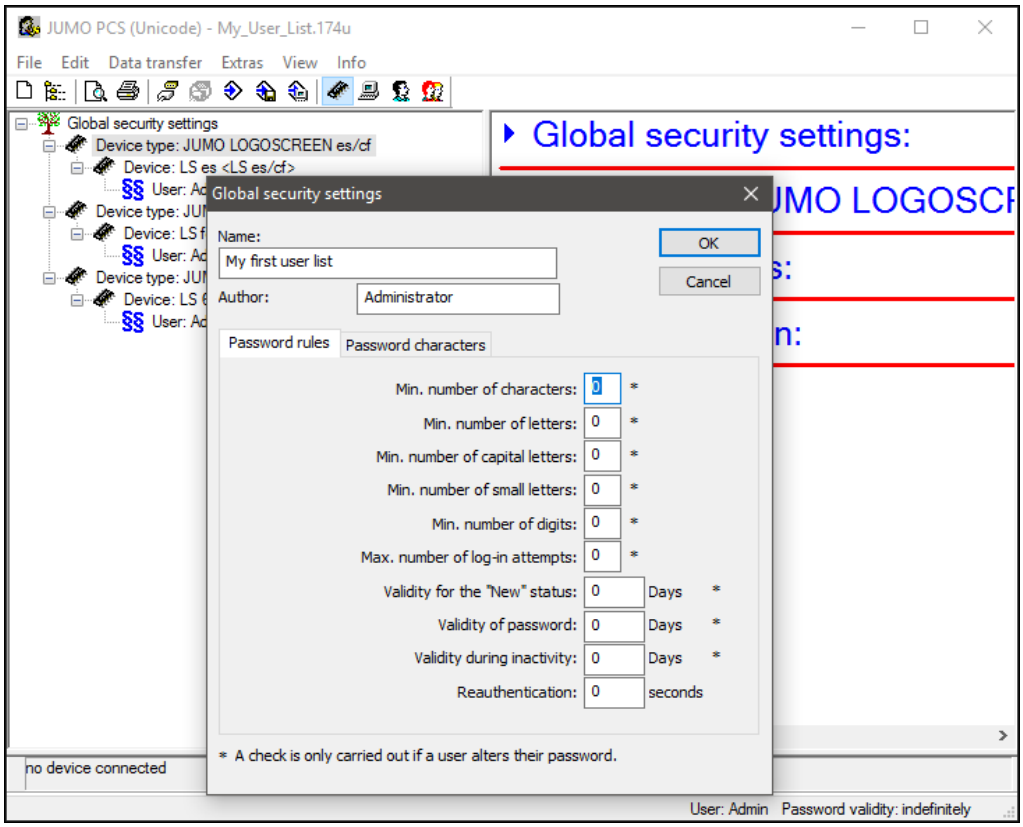
Maximize/minimize

Clicking the "Arrow pointing right" (▶) in front of the entry lists the current dialog windows settings. The entry view is **maximized**.

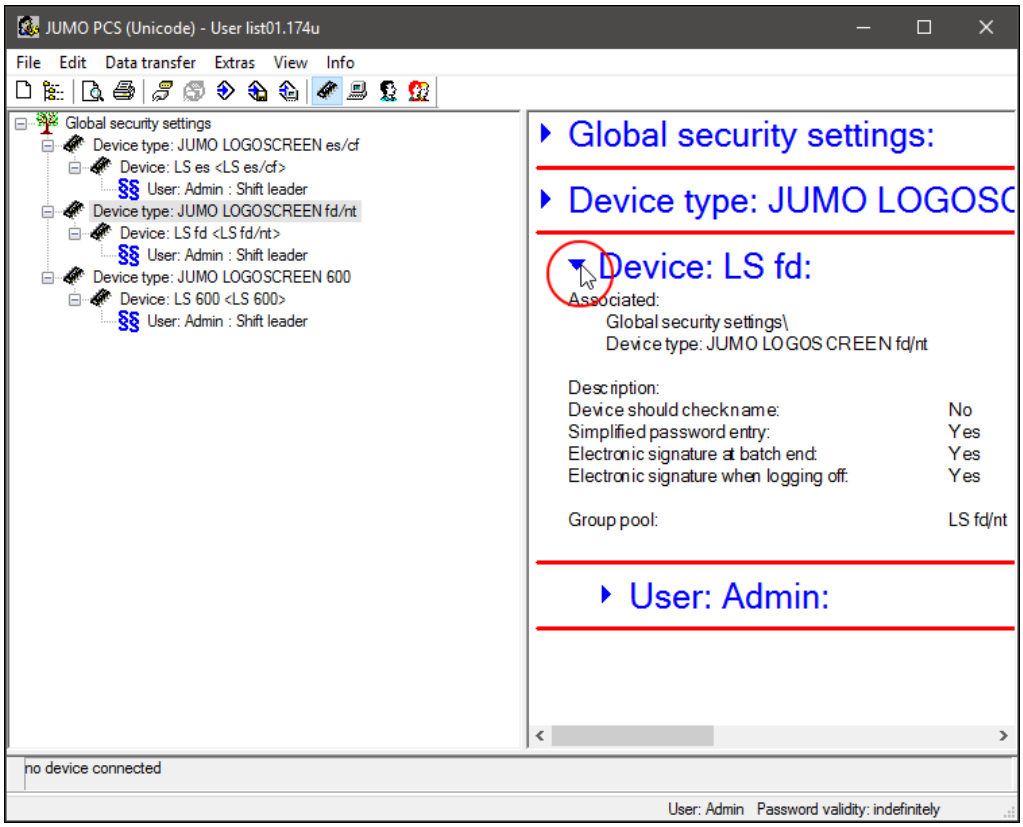
Clicking the "Arrow pointing downward" (▼) hides the current settings again. The entry view is **minimized**.

Alternatively, access the context menu by right-clicking an entry in the dialog window and open the **Maximize/minimize** functions.

Example: Change dialog was started.



Example: List of the current settings.

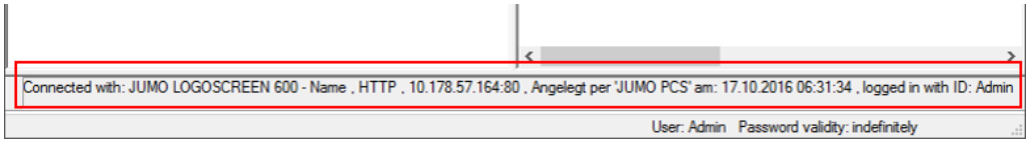


Connection status

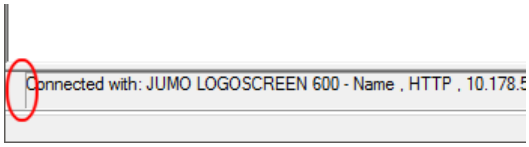
The "Connection status" line indicates whether a connection to a device exists and shows the interface data. The line can also be shown and hidden using the **VIEW > CONNECTION STATUS** function.

Example: No connection

Example: Connection to a device



The line can be moved (like the toolbar):



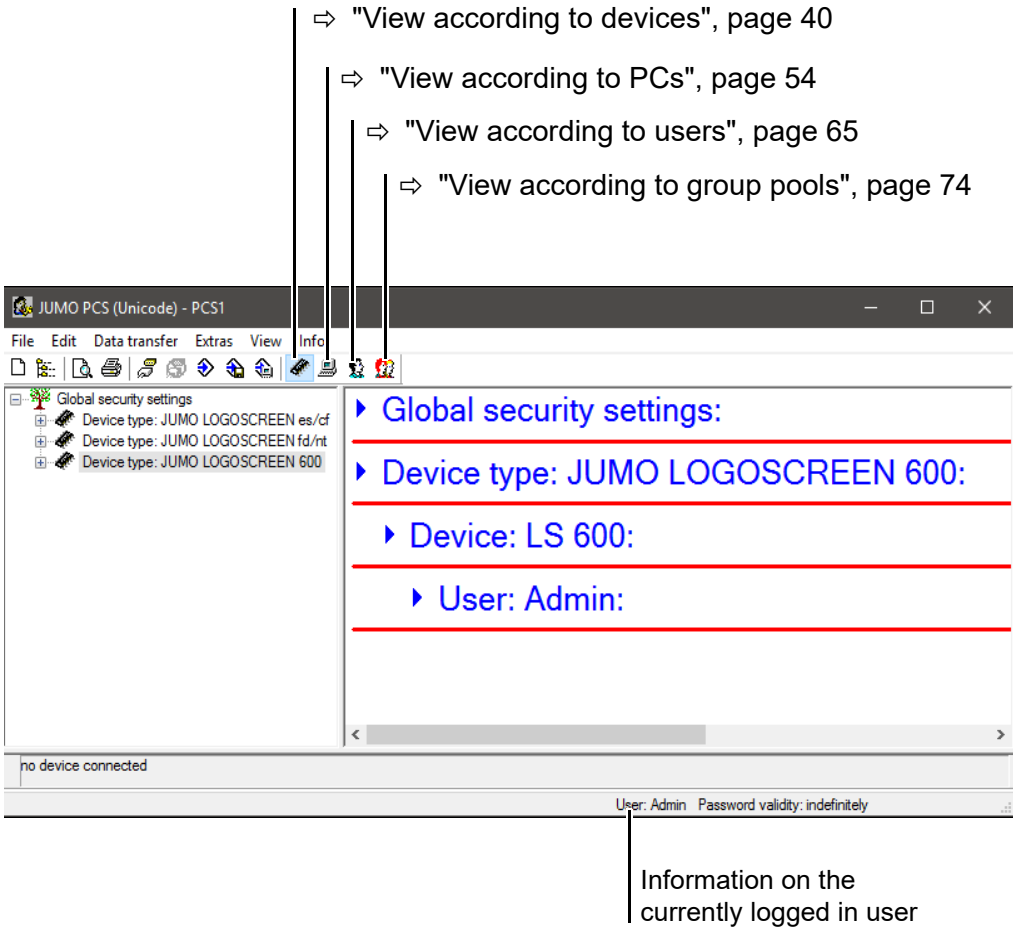
* Move the mouse pointer to the area in front of the text
* Hold the left mouse button and move the mouse
* To fix the line in place again, release the mouse button.

Administrators can assign user rights in user lists and assign them to devices and PCs.

Device and PC rights files are generated from user lists.

Views

In order to edit the user list parameters, five different views can be selected using the **VIEW** command in the menu bar or via the toolbar.



User rights are generated in group pools and assigned/allocated to devices and PCs (programs).

⇨ Chapter 7.5 "View according to group pools"

Device and PC rights file can only be generated in the "According to devices" and "According to PCs" views.

⇨ Chapter 7.2 "View according to devices"

⇨ Chapter 7.3 "View according to PCs"

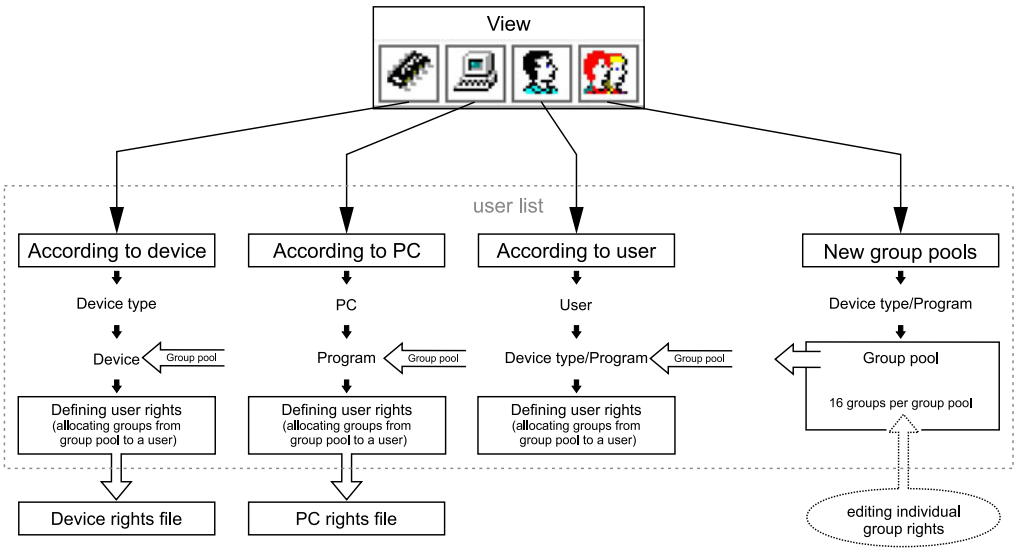
7 Edit user lists

New user lists

The administrator can generate user lists via the user lists wizard.

⇨ Chapter 5 "User lists wizard"

By default, new user lists contain all FDA-compliant JUMO devices and programs, a user (administrator), and device- and program-specific group pools in the respective selected view ("Views", page 37).



The devices, programs and users from a new user list are pre-allocated with device- and program-specific user rights (device- and program rights).

The pre-allocated user rights come from the device- and program-specific rights from the groups of allocated group pools.

New user lists serve as a template for the simple and quick generation of user rights and rights files.

The pre-allocated user rights are stored in the groups of the group pools and are specified via a group assignment for the devices, programs or users.

The user rights can be edited in the respective group pool.

We recommend reading Chapter 7.5 "View according to group pools" before editing new user lists.

User lists from databases

User lists from databases that are generated using profiles can continue to be used and edited.

⇨ Chapter 7.6 "View according to profiles"

7.1 Select view

The view in which the desired function can be executed can be selected via the **VIEW** command in the menu bar or via the toolbar.

Overview of important functions

Functions	Views			
	 "View according to devices", page 40	 "View according to PCs", page 54	 "View according to users", page 65	 "View according to group pools", page 74
Edit global security settings	X	X	X	X
Edit default user rights				X
Create new user rights				X
Assign user rights	X	X	X	
Edit devices available by default	X			
Create new devices	X			
Edit computers available by default		X		
Create new computers		X		
Edit users available by default			X	
Create new users			X	
Edit group pools available by default				X
Create new group pools				X
Generate device rights file	X			
Generate PC rights file		X		

View according to profiles

User lists from databases that contain profiles can continue to be used and edited in the view according to profiles.

Chapter 7.6 "View according to profiles"

7 Edit user lists

7.2 View according to devices

This view shows the (available by default) FDA-compliant device types from a user list.

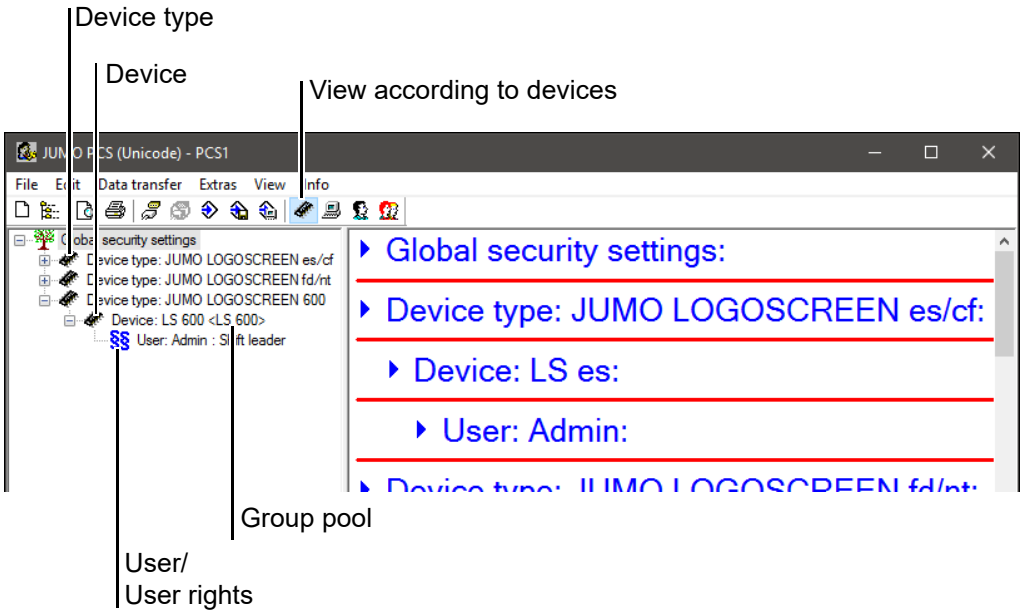
The default user list can be edited as a template to quickly and easily generate a device right file.

⇨ Chapter 7.2.2 "Edit device"

⇨ Chapter 8.2.1 "Generate device rights file"

Open view

✱ Open **VIEW > VIEW ACCORDING TO DEVICES** or press the corresponding button in the toolbar.



Device type By default, all FDA-compliant "device types" are created in each new user list.

Device A "device" is assigned to each device type by default.

Group pool Each device is pre-allocated with a device-specific group pool by default.

⇨ Chapter 7.5 "View according to group pools"

User rights The user (administrator) that was created via the **USER LISTS WIZARD** during installation is allocated to each device (Chapter 5.2 "Define administrator").

Device-specific user rights are assigned to this user from the group pool created by default.

7.2.1 Functions in the view according to devices

The following functions can be executed in this view:

- **Edit global security settings**

⇨ Chapter 5.6.1 "Edit global security settings"

- **Edit devices available by default**

⇨ Chapter 7.2.2 "Edit device"

- **Create new devices**

⇨ Chapter 7.2.3 "New device"

- **Assign user rights available by default**

⇨ Chapter 7.2.4 "User group assignment: edit"

- **Assign new user rights**

⇨ Chapter 7.2.5 "New user rights"

- **Edit user settings**

⇨ Chapter 7.2.6 "Edit users"

- **Remove devices and user rights**

⇨ Chapter 7.2.7 "Remove"

- **Generate a user rights file from the user list**

⇨ Chapter 8.2.1 "Generate device rights file"

- **Transfer a user list to the device as a device rights file**

⇨ Chapter 8.1.6 "Device rights file for the device"

- **General functions in this view**

⇨ Chapter 7.2.8 "General functions in this view"

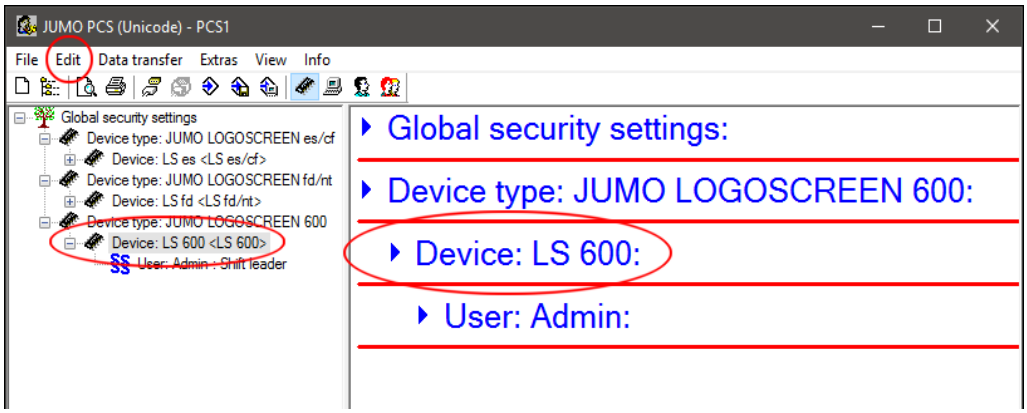
7.2.2 Edit device

If devices available by default or newly created devices are used as a template for generating device rights files, they can be subsequently edited.

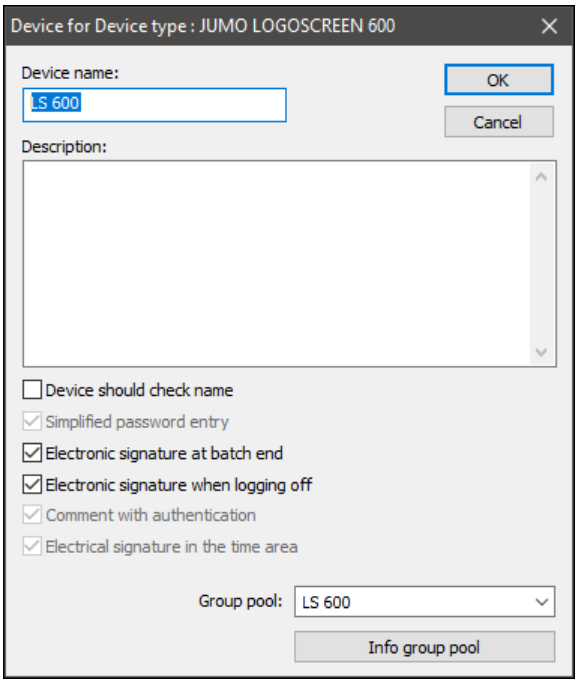
Edit device features

* Select the corresponding "device" in the navigation tree and invoke the **Device: edit** command using the right mouse button.

Alternatively, select the corresponding "device" in the dialog window and invoke the **Device: edit** command using the right mouse button or invoke the **EDIT > DEVICE: EDIT** command via the menu bar.



The following dialog window opens:



Device name

* Enter the device name.

It should be identical to the name that was also entered in the device via the **CONFIGURATION > DEVICE DATA > DEVICE DESIGNATION** parameters.

Description

* A device description can also optionally be added, e.g. a brief functional description.

Device should check name

The device name on the file is compared with the device name on the device when integrating a device rights file in a device. The device only accepts the device rights file if they are identical.

If enabled (☑), this option prevents the file from being integrated in an incorrect device.

Simplified password entry

If this option is enabled (☑), the password is entered on the device using the soft keys. If the option is disabled, the password is entered using the standard editor on the respective device.

Important information about the password entry on the device used can be found in the respective device-specific operating manual.

Electronic signature for batch end

The option is enabled by default (☑). The end of a batch reporting process **can** involve an electronic signature. The signature is provided with the date and time in the device audit trail and can be evaluated using the PC Evaluation Software (PCA3000).

Electronic signature when logging off

The option is enabled by default (☑). The user **must** provide an electronic signature on the device when logging off. The signature is provided with the date and time in the device audit trail and can be evaluated using the PC Evaluation Software (PCA3000).

Comment with authentication

When this option is enabled (☑), any user who has the appropriate authorization ("View recording data and evaluate history" right) can make a comment with authentication. This can be another user than the one who is currently logged on.

Electronic signature for time range

When this option is enabled (☑), a certain time range in the device can be provided with an electronic signature. The signature applies to the time range that is displayed in the diagram at the time of the signature.

Group pool

In the new user lists, a group pool is assigned to each FDA-compliant device by default, e.g. **<LS 600>** for the device "LS 600".

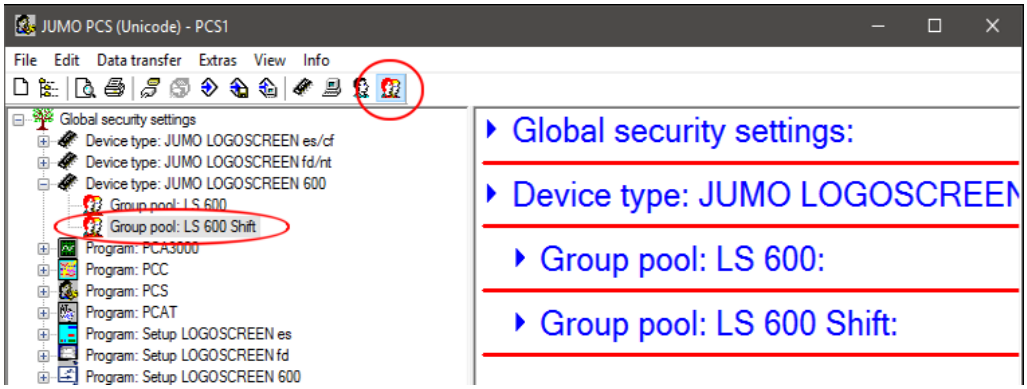
This group pool provides the device-specific and program-specific rights that can be allocated respectively to the users created by default (administrators) or to each new user.

7 Edit user lists

Allocate/change the group pool

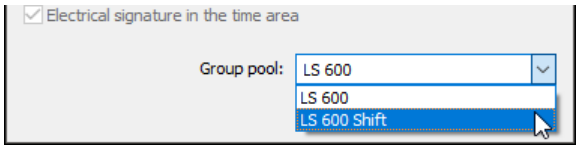
If rights other than those available by default in the group pool need to be assigned to a user, a new group pool must first be created for this program.

⇨ Chapter 7.5.3 "New group pool"



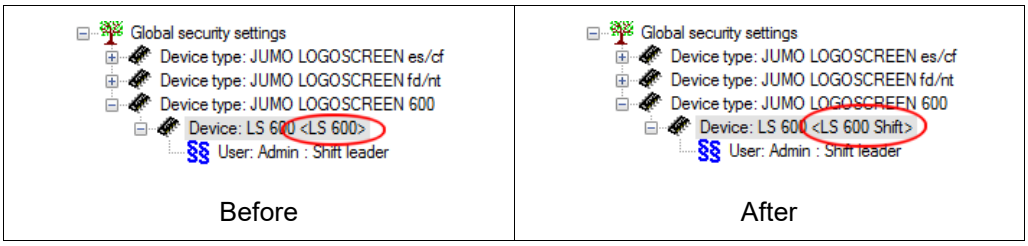
The newly created group pool can then be allocated to the program:

* Switch back to the **View according to devices**.
* Select the "device" in the navigation tree and invoke the **Device: edit** command using the right mouse button.
* Select the desired group pool from the drop-down menu.



*Confirm the selection using the OK button.

A new group pool is allocated to the device.

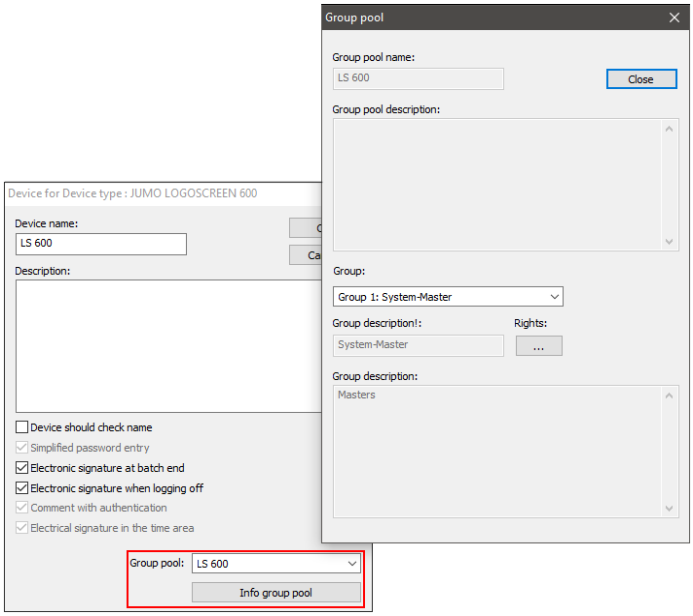


User rights from the groups in the new group pools can then be allocated to the device.

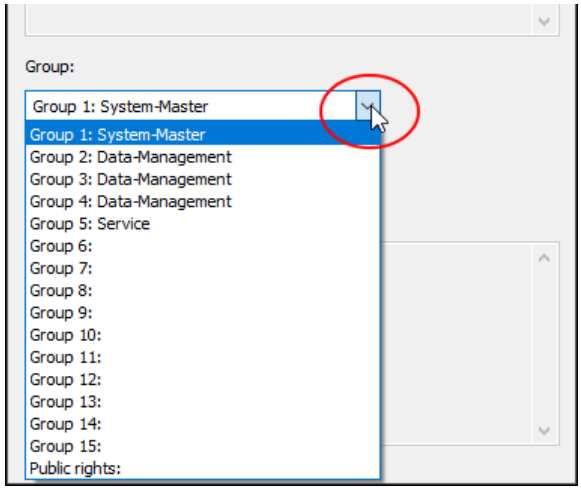
⇨ Chapter 7.2.4 "User group assignment: edit"

Info group pool

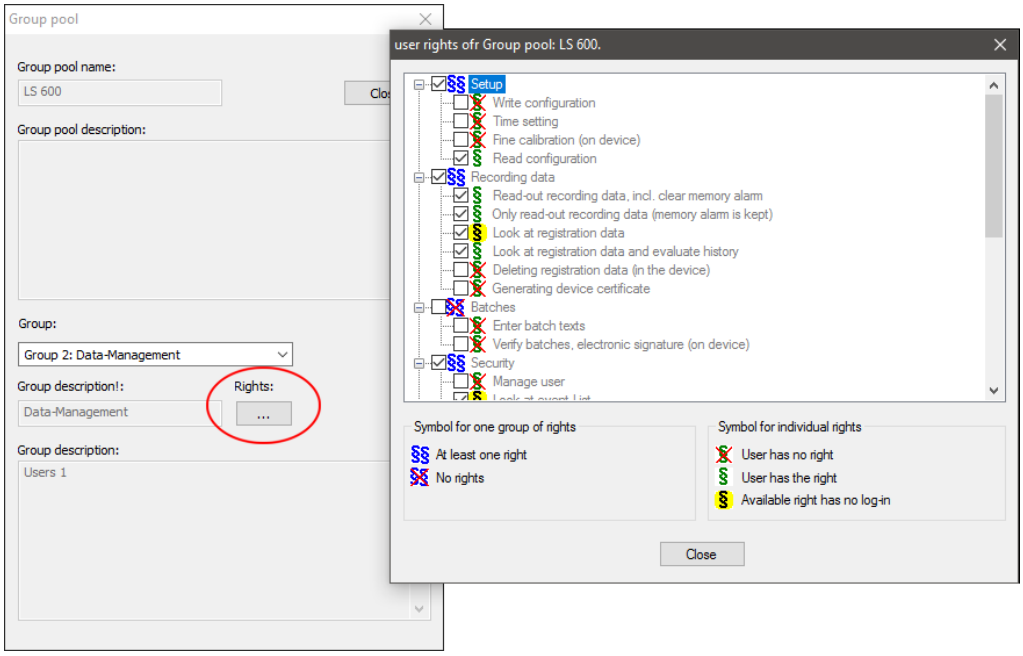
Details about the rights for the respective group can be displayed using the **INFO GROUP POOL** button.



✱ Select the desired group (user role) from the **Group** drop-down menu.



* The **RIGHTS** button opens a view window with an overview of the user rights for the selected group.



The user rights are specified in the "View according to group pools", page 74 and are only displayed here.

The user rights cannot be edited in this dialog.

Expanding and limiting rights to a group (user rights) in the group pool:

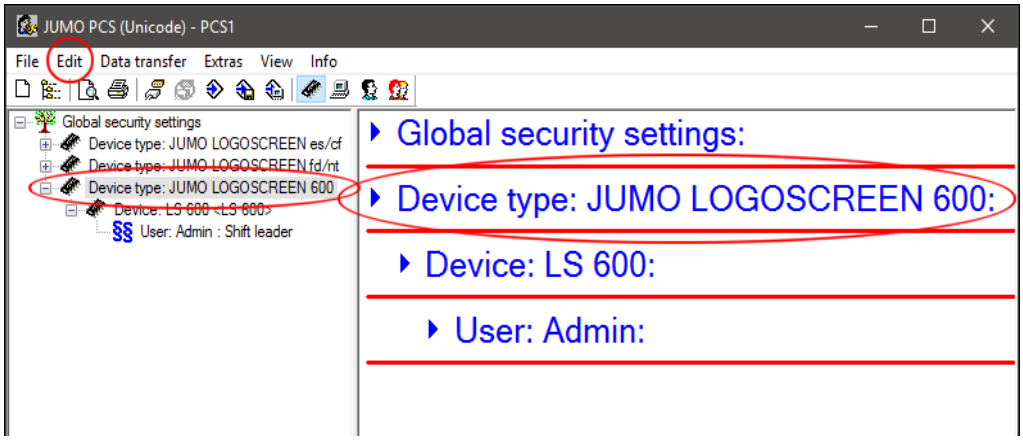
⇨ "Edit user rights", page 79

7.2.3 New device

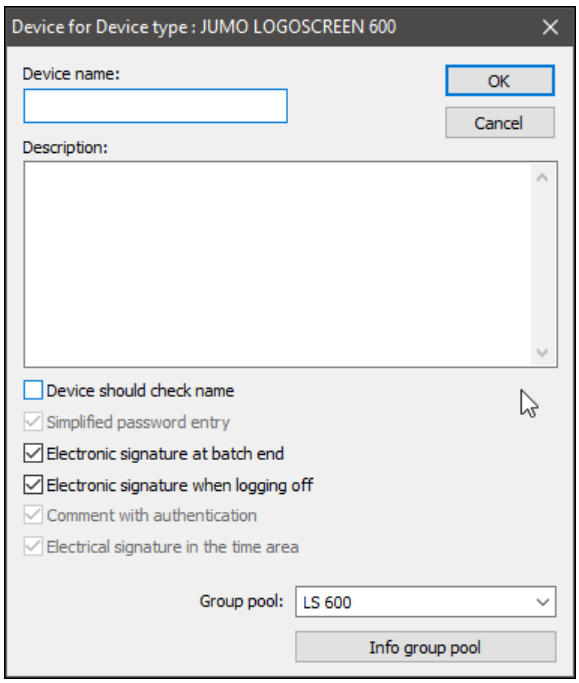
Create new device

* Select the corresponding "device type" in the navigation tree and invoke the **New device** command using the right mouse button.

Alternatively, select the corresponding "device type" in the dialog window and invoke the **New device** command using the right mouse button or invoke the **EDIT > NEW DEVICE** command via the menu bar.



The following dialog window opens:



* Then provide the necessary information about the device to be created

The further course of action for creating a new device is the same as in Chapter 7.2.2 "Edit device".

7.2.4 User group assignment: edit

Groups available by default or newly created groups (user rights) can be assigned to or removed from a user.

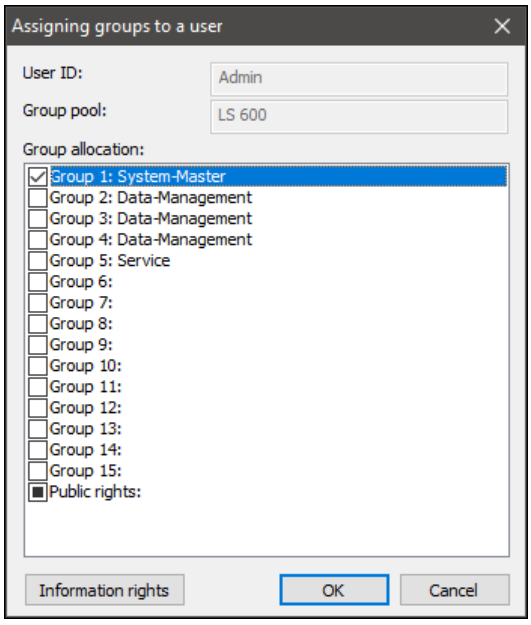
Any change to the user rights in this view may also affect previously assigned device rights for this device in the **View according to users** (Page 65).

Allocate groups (user rights)

* Select the corresponding "user" in the navigation tree and invoke the **User group assignment: edit** command using the right mouse button.

Alternatively, select the corresponding "user" in the dialog window and invoke the **User group assignment: edit** command using the right mouse button or invoke the **EDIT > USER GROUP ASSIGNMENT: EDIT** command via the menu bar.

The following dialog window opens:



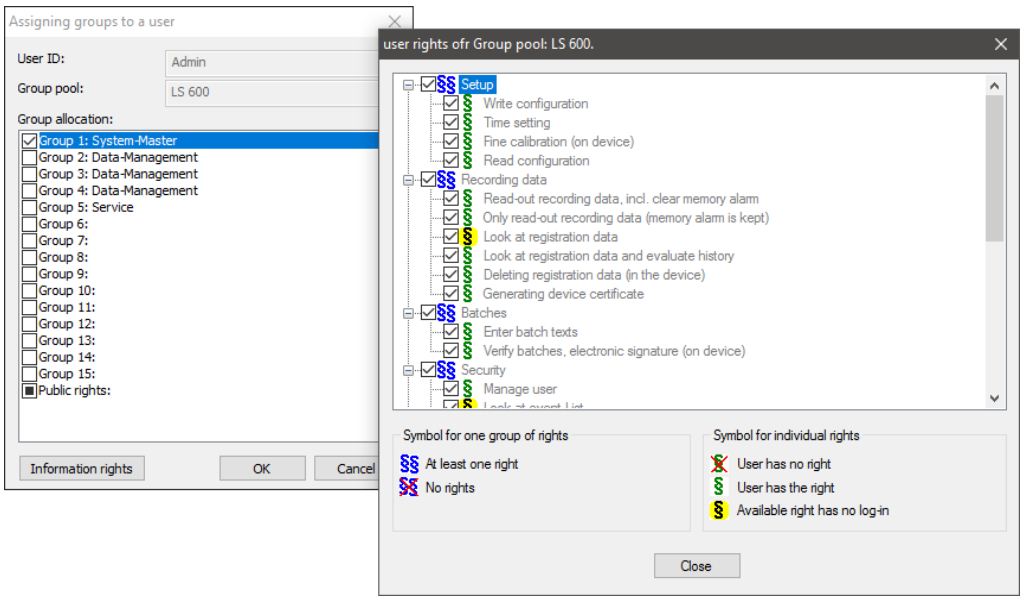
* Allocate groups or remove them from the respective user by enabling (☑) or disabling (☐) this option, and confirm using the OK button.

User rights, which were determined for the respective group via **VIEW > VIEW ACCORDING TO GROUP POOLS** ("Edit user rights", page 79), are thus defined for the user via the group assignment ("Information rights", page 49).

If more than one group with user rights is allocated to the user, the groups and their user rights are logically OR-linked and thus yield the whole rights situation.

Information rights

* The **INFORMATION RIGHTS** button opens a view window with an overview of the user rights for the selected group.



The user rights are specified in the "View according to group pools", page 74 and are only displayed here

The user rights cannot be edited in this dialog.

Expanding and limiting rights to a group (user rights) in the group pool:

⇨ "Edit user rights", page 79

7 Edit user lists

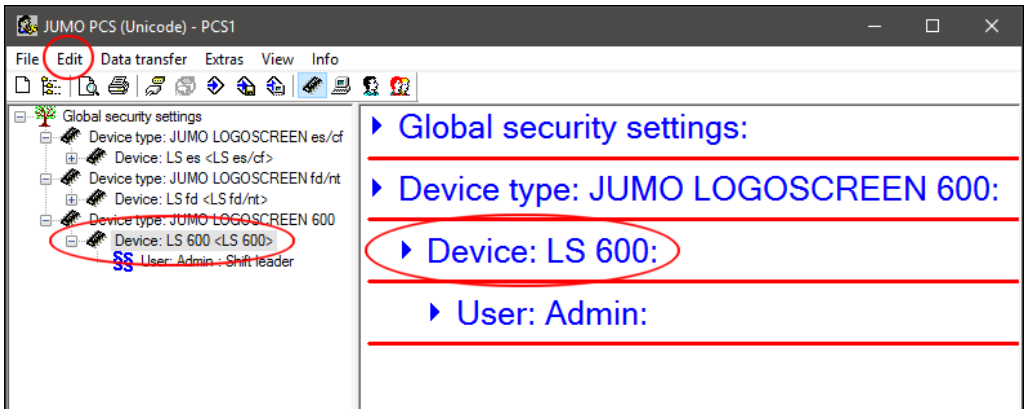
7.2.5 New user rights

New user rights for all available users (Chapter 7.4 "View according to users") can be assigned to each device.

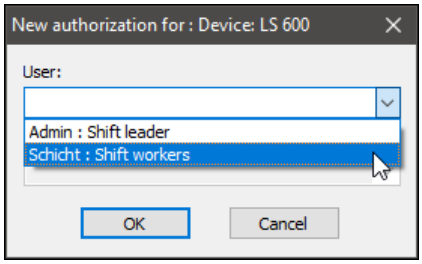
Allocate new user rights

* Select the corresponding "device" in the navigation tree and invoke the **New user rights** command using the right mouse button.

Alternatively, select the corresponding "device" in the dialog window and invoke the **New user rights** command using the right mouse button or invoke the **EDIT > NEW USER RIGHTS** command via the menu bar.



* Select the user in the following dialog and confirm using the OK button.



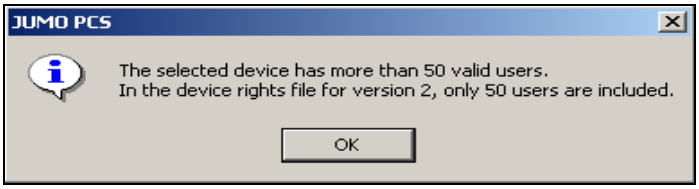
.

The further course of action for allocating new user rights is the same as in Chapter 7.2.4 "User group assignment: edit".

Max. number of users

Device user lists (device rights files) must be transferred to the corresponding devices so that the users are available there and can log on.

If more than 50 users are assigned to a device, only 50 are sent to the device.

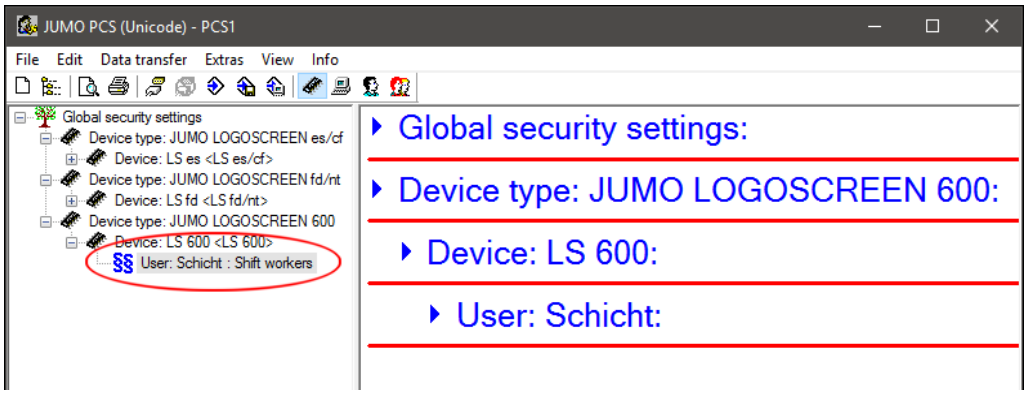


⇨ Chapter 8 "Data transfer to the device"

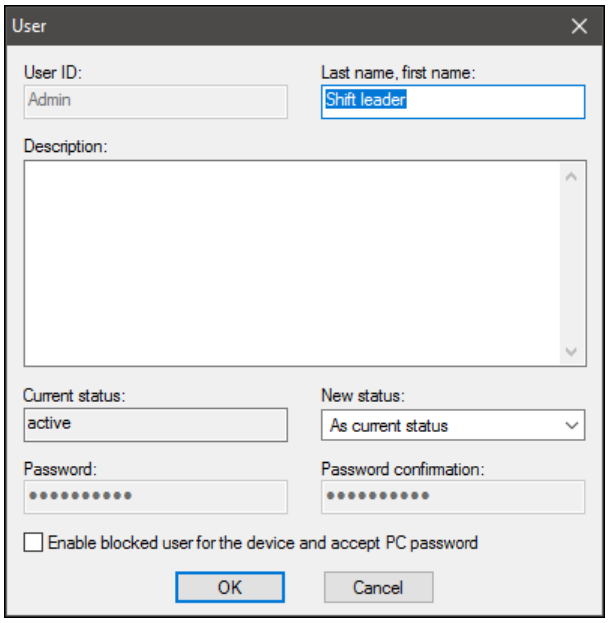
- Blocked users are not accepted in the device rights file.
- At least one (1) user must have the "Manage users" device right, otherwise the device rights file cannot be sent to the device.

7.2.6 Edit users

✱ Select the corresponding "user" in the navigation tree and invoke the **Users: edit** command using the right mouse button.



The following dialog window opens:



The further course of action for editing the user settings is the same as the description in the **View according to users**.

⇨ Chapter 7.4.2 "Edit users"

7.2.7 Remove

Remove device

Removes the device incl. all assigned user and the associated user rights (groups) from the list.

* Select the corresponding "device" in the navigation tree and invoke the **Remove device** command using the right mouse button.

User group assignment: remove

Removes the selected user and the associated user rights (groups) from the list.

* Select the corresponding "user" in the navigation tree and invoke the **User group assignment: remove** command using the right mouse button.

The "Global security settings" and "Device type" entries cannot be removed.

7.2.8 General functions in this view

The following functions can be accessed in this view using the right mouse button (context menu) in all entries of the navigation tree and the dialog window.

Expand node

⇨ "Expand/collapse node", page 34

Collapse node

⇨ "Expand/collapse node", page 34

Maximize/minimize device type

⇨ "Maximize/minimize", page 34

Copy device type to clipboard

The information listed in the dialog window about the device type is copied to the clipboard and can be added, e.g. in a text-processing program.

Copy everything to clipboard

Copies all information in the dialog window concerning general safety provisions, device type, device and users to the clipboard.

Print

"Print", page 119

7 Edit user lists

7.3 View according to PCs

This view shows the FDA-compliant programs (available by default) in a user list.

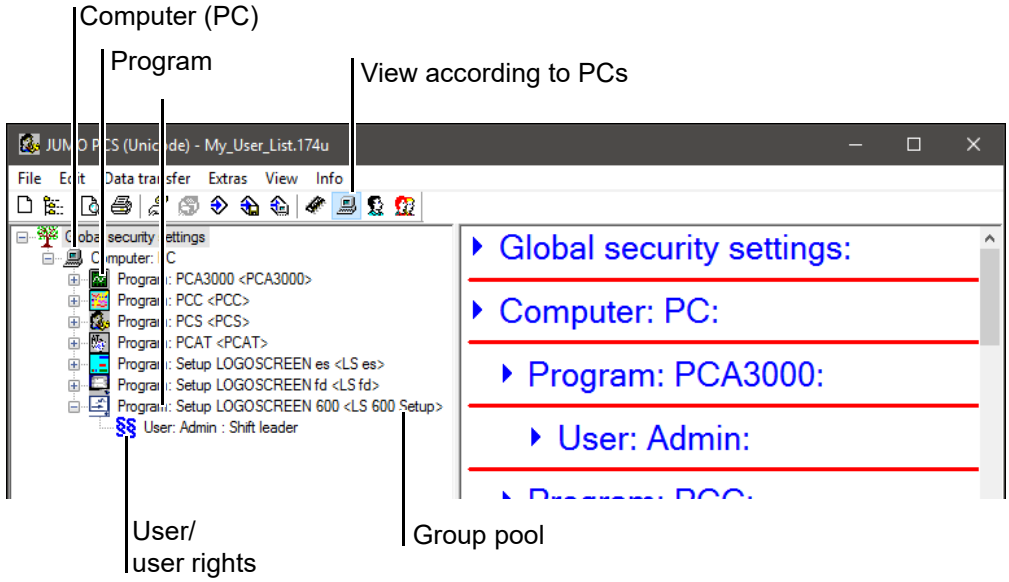
The default user list can be edited as a template for the quick and simple generation of a PC rights file.

⇨ Chapter 7.3.2 "Edit computer (PC)"

⇨ Chapter 7.9.2 "Generate PC rights file"

Open view

✱ Open the **VIEW > VIEW ACCORDING TO PCS** menu or press the corresponding button in the toolbar.



Computer

A computer (PC) is already created by default in each new user list.

Program

All FDA-compliant "programs" are assigned by default to the created computer (PC).

Group pool

Each program is pre-allocated by default with a program-specific group pool.

⇨ Chapter 7.5 "View according to group pools"

User rights

The user (administrator) that was created during the installation via the **USER LISTS WIZARD** is assigned to each program (Chapter 5.2 "Define administrator").

Program-specific user rights from the group pool created by default are allocated to this user.

7.3.1 Functions in the view according to PCs

The following functions can be executed in this view:

- **Edit global security settings**

⇨ Chapter 5.6.1 "Edit global security settings"

- **Edit computers (PCs) available by default**

⇨ Chapter 7.3.2 "Edit computer (PC)"

- **Create new PCs**

⇨ Chapter 7.3.3 "New PC"

- **Edit programs**

⇨ Chapter 7.3.4 "Edit program"

- **Assign user rights available by default**

⇨ Chapter 7.3.5 "User group assignment: edit"

- **Assign new user rights**

⇨ Chapter 7.3.6 "New user rights"

- **Edit user settings**

⇨ Chapter 7.3.7 "Edit users"

- **Remove PCs and user rights**

⇨ Chapter 7.3.8 "Remove"

- **Generate a PC rights file from the user list**

⇨ Chapter 8.2.1 "Generate device rights file"

- **Transfer a user list to the device as a device rights file**

⇨ Chapter 9.2.2 "Generate PC rights file"

- **General functions in this view**

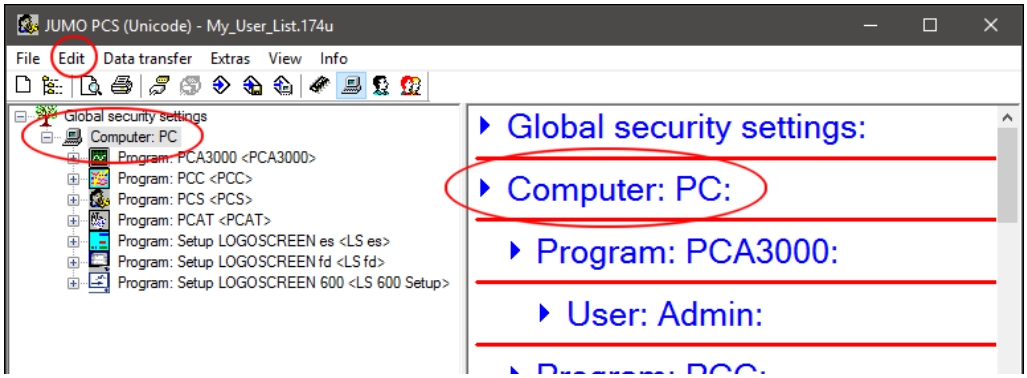
⇨ Chapter 7.3.9 "General functions in this view"

7.3.2 Edit computer (PC)

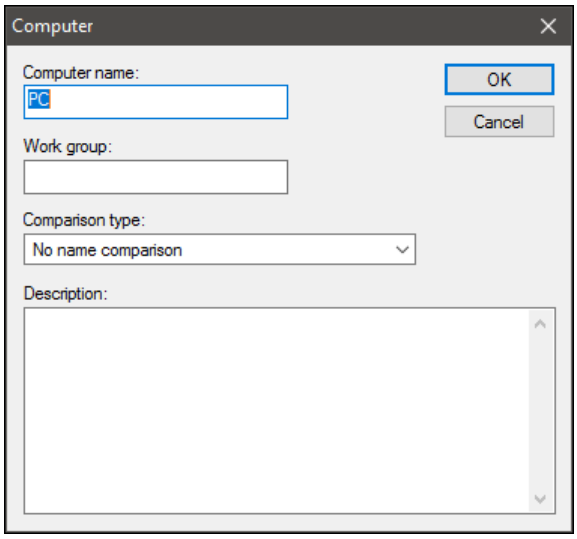
If computers (PCs) available by default or newly created devices are used as a template for generating device rights files, they can be subsequently edited.

✱ Select the corresponding "computer" in the navigation tree and invoke the **Computer: edit** command using the right mouse button.

Alternatively, select the corresponding "computer" in the dialog window and invoke the **Computer: edit** command using the right mouse button or invoke the **EDIT > COMPUTER: EDIT** command via the menu bar.



The following dialog window opens:

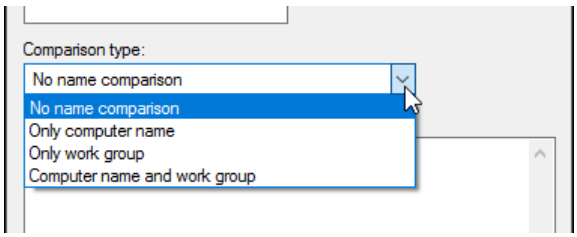


Computer name The name "PC" is specified by default for the computer in a new user list. A computer name **must** be provided. The name can be edited if it needs to be used as a **comparison type** (Page 57).

Work group No work group is specified by default for the computer in a new user list. A work group **can** be entered if it is to be used as a **comparison type** (Page 57).

Comparison type

When the comparison type is enabled, a user list can only be used for the PCs and/or in work groups that match the comparison. The comparison takes place between the user list and the PC that accesses this user list.



No name comparison

If the user list is stored on a network PC for example, no name comparison takes place when accessing the user list from a PC.

Only computer name

If the user list is given a specific computer name (Page 56) and is stored on a network PC for example, only PCs with the same name can access this user list.

Only work group

If the user list is assigned to a specific work group (Page 56) and is stored on a network PC for example, only work groups with the same name can access this user list.

Computer name and work group

If the user list is given a specific computer name (Page 56), assigned to a specific work group and stored on a network PC for example, only PCs with the same name with work groups with the same name can access this user list.

Description

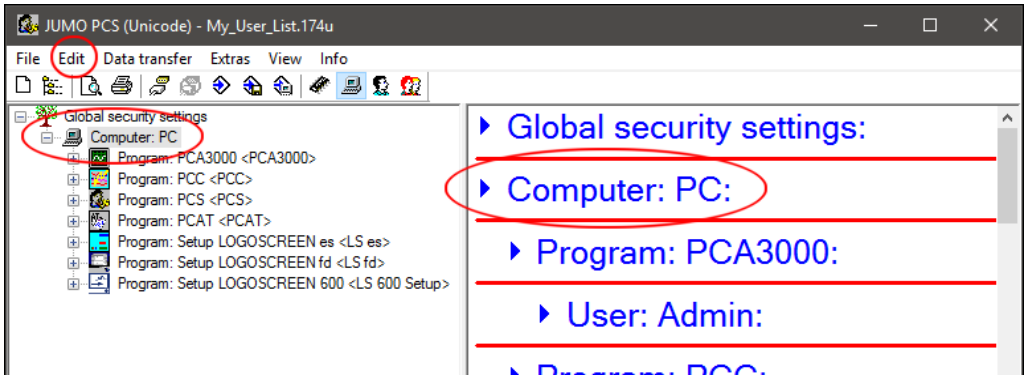
A precise description of the computer (PC) can be entered in this field, e.g. the location.

7.3.3 New PC

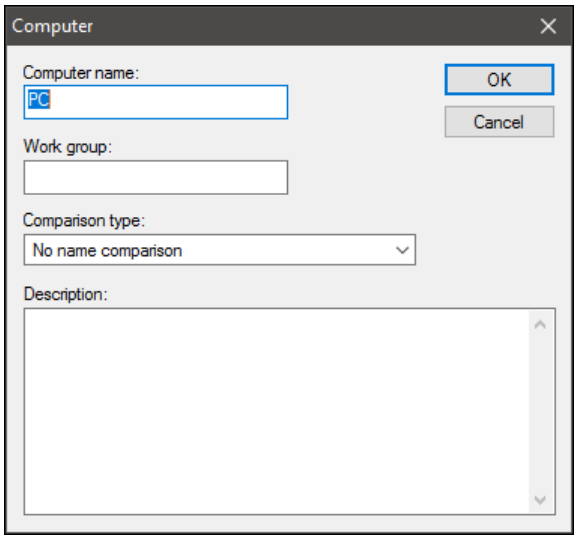
Create new PC (computer)

* Select a "computer" in the navigation tree and invoke the **New PC** command using the right mouse button.

Alternatively, select a "computer" in the dialog window and invoke the **New PC** command using the right mouse button or invoke the **EDIT > NEW PC** command via the menu bar.



The following dialog window opens:

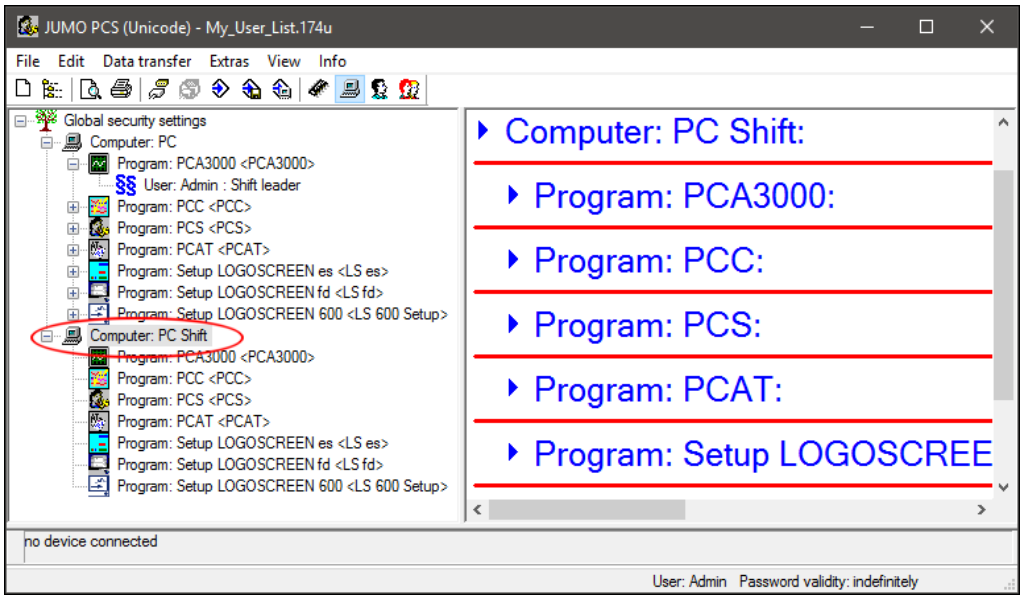


* Then provide the necessary information about the PC to be created.

The further course of action for creating a new PC is the same as in Chapter 7.3.2 "Edit computer (PC)".

* Complete the entries using the OK button.

A new PC has been created with all the FDA-compliant programs.



First, the default program-specific group pools are allocated to a new PCs FDA-compliant programs.

No user rights are allocated to the programs yet. This must be performed in the next work step.

⇨ Chapter 7.3.6 "New user rights"

7.3.4 Edit program

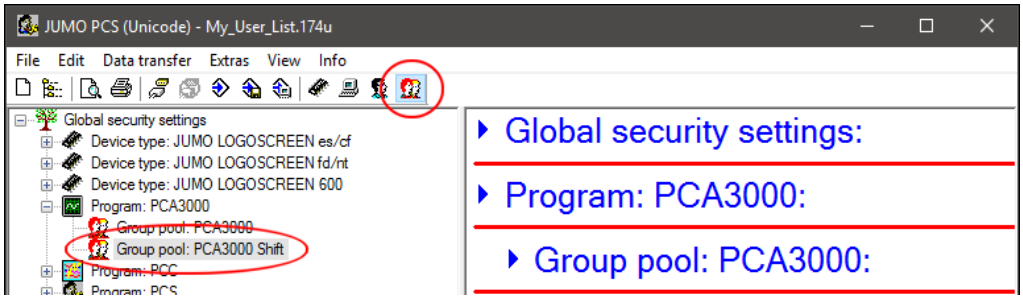
In the new user lists and with newly created PCs, a group pool is assigned to each FDA-compliant program by default, e.g. <PCA3000> for the program "PCA3000".

This group pool provides the program-specific rights that can be allocated respectively to the users created by default (administrators) or to each new user.

Allocate/change the group pool

If other rights need to be assigned to the user of a program than those available by default in the group pool, a new group pool must first be created for this program.

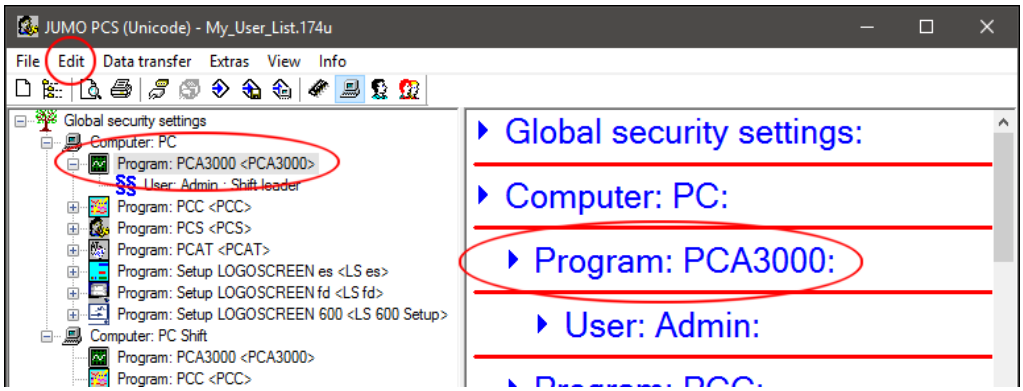
⇨ Chapter 7.5.3 "New group pool"



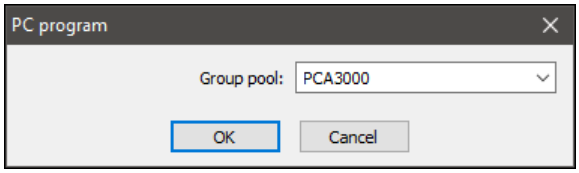
The newly created group pool can then be allocated to the program:

* Switch back to the **View according to PCs** if necessary
* Select the "program" in the navigation tree and invoke the **Program: edit** command using the right mouse button.

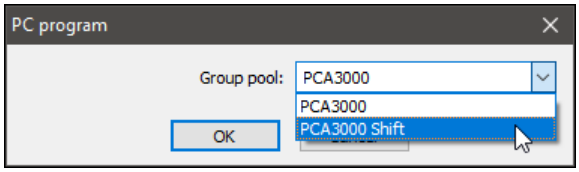
Alternatively, select the "program" in the dialog window and invoke the **Program: edit** command using the right mouse button or invoke the **EDIT > PROGRAM: EDIT** command via the menu bar.



The following dialog window opens:



* Select the desired group pool from the drop-down menu.



* Confirm the selection using the OK button.

A new group pool is allocated to the program.

User rights from the groups of the new group pools can then be allocated to the program.

⇨ Chapter 7.3.5 "User group assignment: edit"

7.3.5 User group assignment: edit

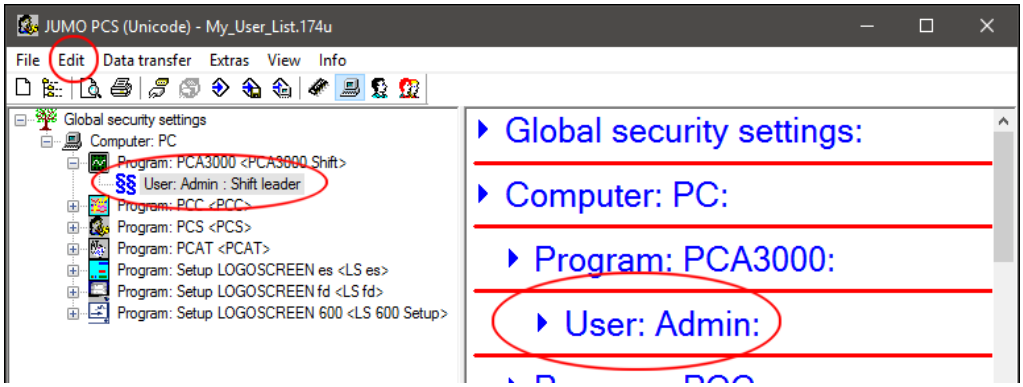
Groups available by default or newly created groups (user rights) can be assigned to or removed from each user.

Any change to the user rights in this view may also affect previously assigned program rights for this program in the **View according to users** (Page 65).

Allocate groups (user rights)

* Select the corresponding "user" in the navigation tree and invoke the **User group assignment: edit** command using the right mouse button.

Alternatively, select the corresponding "user" in the dialog window and invoke the **User group assignment: edit** command using the right mouse button or invoke the **EDIT > USER GROUP ASSIGNMENT: EDIT** command via the menu bar.



The further course of action is the same as the description in the **View according to devices**.

⇨ Chapter 7.2.4 "User group assignment: edit"

7 Edit user lists

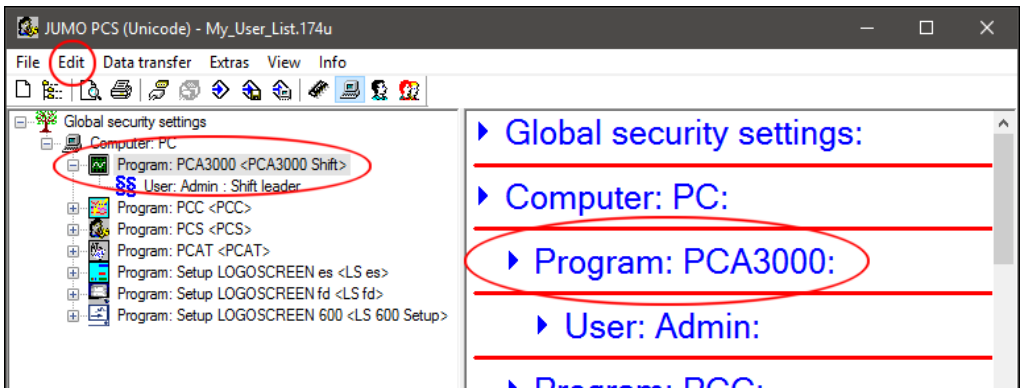
7.3.6 New user rights

New user rights for all available users (Chapter 7.4 "View according to users") can be assigned to each PC.

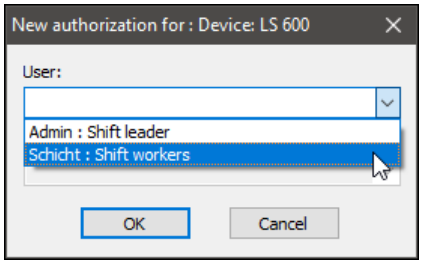
Allocate new user rights

* Select the corresponding "program" in the navigation tree and invoke the **New user rights** command using the right mouse button.

Alternatively, select the corresponding "program" in the dialog window and invoke the **New user rights** command using the right mouse button or invoke the **EDIT > NEW USER RIGHTS** command via the menu bar.



* Select the user in the following dialog and confirm using the OK button.

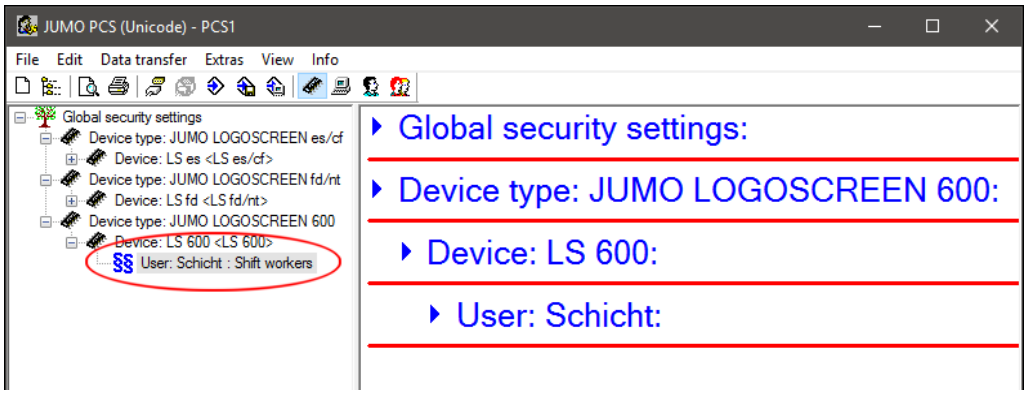


The further course of action for allocating new user rights is the same as the description in the **View according to devices**.

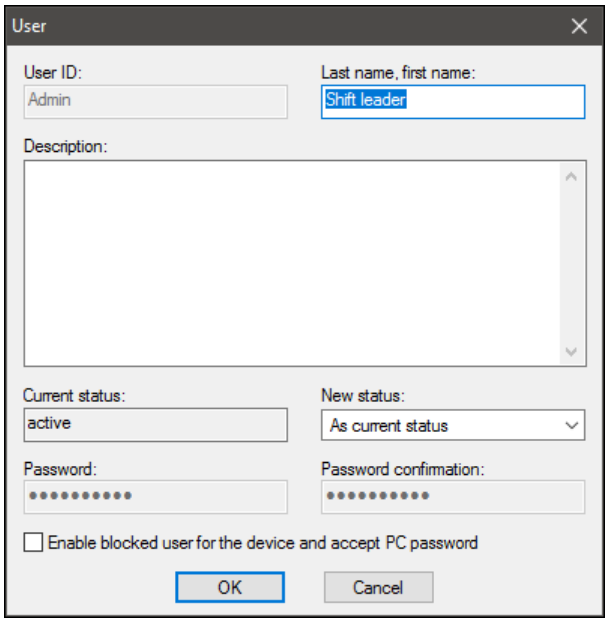
⇨ Chapter 7.2.4 "User group assignment: edit"

7.3.7 Edit users

✱ Select the corresponding "user" in the navigation tree and invoke the **Users: edit** command using the right mouse button.



The following dialog window opens:



The further course of action is the same as the description in the **View according to users**.

⇨ Chapter 7.4.2 "Edit users"

7.3.8 Remove

Computer: remove

Removes the selected computer incl. all assigned programs and users and the associated user rights (groups) from the list.

✱ Select the corresponding "computer" in the navigation tree and invoke the **Computer: remove** command using the right mouse button.

Program authorizations: remove

Removes all the users assigned to the program and the associated user rights (groups) from the list.

* Select the corresponding "program" in the navigation tree and invoke the **Program authorizations: remove** command using the right mouse button.

User group assignment: remove

Removes the selected user and the associated user rights (groups) from the list.

* Select the corresponding "user" in the navigation tree and invoke the **User group assignment: remove** command using the right mouse button.

The "Global security settings" and "Device type" entries cannot be removed.

7.3.9 General functions in this view

The following functions can be accessed in this view using the right mouse button (context menu) in all entries of the navigation tree and the dialog window.

Expand node

⇨ "Expand/collapse node", page 34

Collapse node

⇨ "Expand/collapse node", page 34

Maximize/minimize computer/program

⇨ "Maximize/minimize", page 34

Copy computer/program to clipboard

The information listed in the dialog window about the computer/program is copied to the clipboard and can be added, e.g. in a text-processing program.

Copy everything to clipboard

Copies all information in the dialog window concerning general safety provisions, computer, program and users to the clipboard.

Print

"Print", page 119

7.4 View according to users

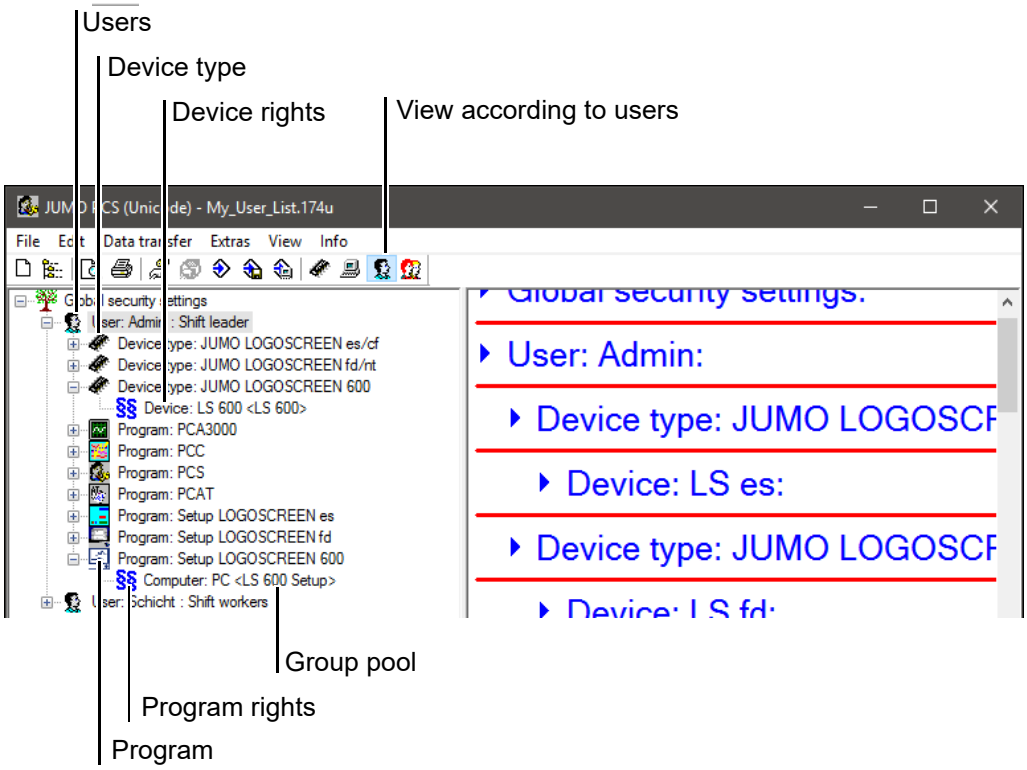
This view shows the users (available by default) of a user list.

The default user list can be edited as a template to quickly and easily generate device and program rights.

⇨ Chapter 7.4.4 "Device/computer group assignment: edit"

Open view

* Open the **VIEW > VIEW ACCORDING TO USERS** menu or press the corresponding button in the toolbar.



Users

A user is already created by default in each new user list.

⇨ Chapter 5.2 "Define administrator"

Device type/ program

All FDA-compliant "device types" and "programs" are assigned by default to the created user (administrator).

Group pool

Each device type or each program is pre-allocated by default with a device-specific or program-specific group pool.

⇨ Chapter 7.5 "View according to group pools"

Device rights/ program rights

Device rights or program rights are allocated to each device type/program. These rights correspond to the respective user rights in the **View according to devices** (Page 40) or the **View according to PCs** (Page 54).

7.4.1 Functions in the view according to users

The following functions can be executed in this view:

- **Edit global security settings**

⇨ Chapter 5.6.1 "Edit global security settings"

- **Edit users available by default**

⇨ Chapter 7.4.2 "Edit users"

- **Create new users**

⇨ Chapter 7.4.3 "New user"

- **Assign device and program rights available by default**

⇨ Chapter 7.4.4 "Device/computer group assignment: edit"

- **Assign new device and program rights**

⇨ Chapter 7.4.5 "New device/program rights"

- **Remove device and program rights**

⇨ Chapter 7.4.6 "Remove"

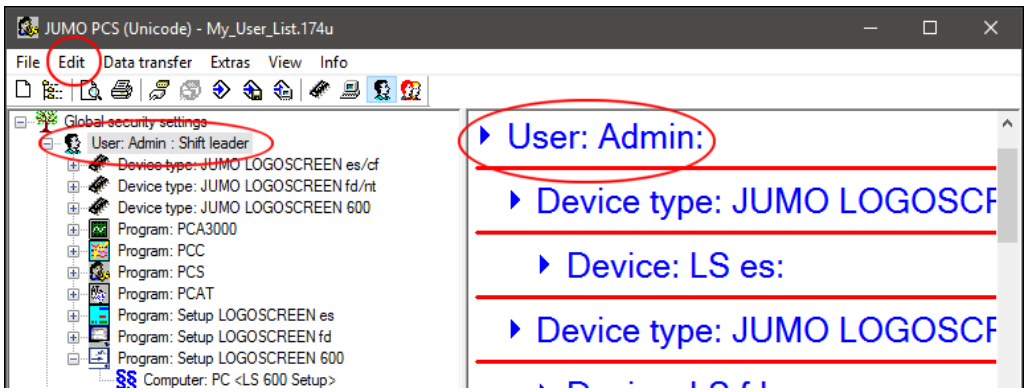
- **General functions in this view**

⇨ Chapter 7.4.7 "General functions in this view"

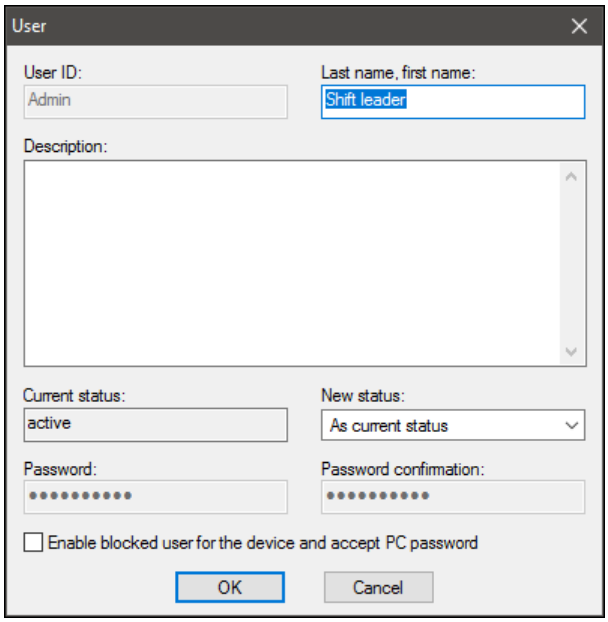
7.4.2 Edit users

✱ Select the corresponding "user" in the navigation tree and invoke the **Users: edit** command using the right mouse button.

Alternatively, select the corresponding "user" in the dialog window and invoke the **User: edit** command using the right mouse button or invoke the **EDIT > USER: EDIT** command via the menu bar.



The following dialog window opens:

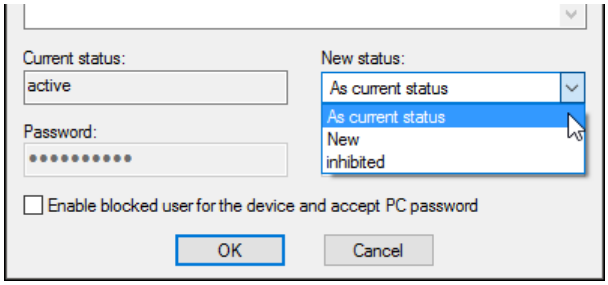


Last name, first name

Last name and first name are determined when generating a new user list using the user lists wizard (Chapter 5.2 "Define administrator"). This designation can be altered here.

New status

If the user status needs to be preserved or changed, this can be selected via the drop-down menu:



⇨ "Validity for the status "New"", page 23

Blocked (block user)

The administrator can block the user for this user list via **Blocked**.

Blocked users are not accepted in the device rights file.

⇨ "Max. number of users", page 51

Release blocked users

The administrator can release the blocked user again for this user list via **New**.

The user released by the administrator muss log on to the device/ program again and is prompted to change their password.

⇨ Chapter 5.4 "Options for program start"

Release blocked users in the device...

By enabling (☑) this option, the administrator cam release the user in the device again if this user was blocked due to, for example, an infringement of the password rules (Page 22).

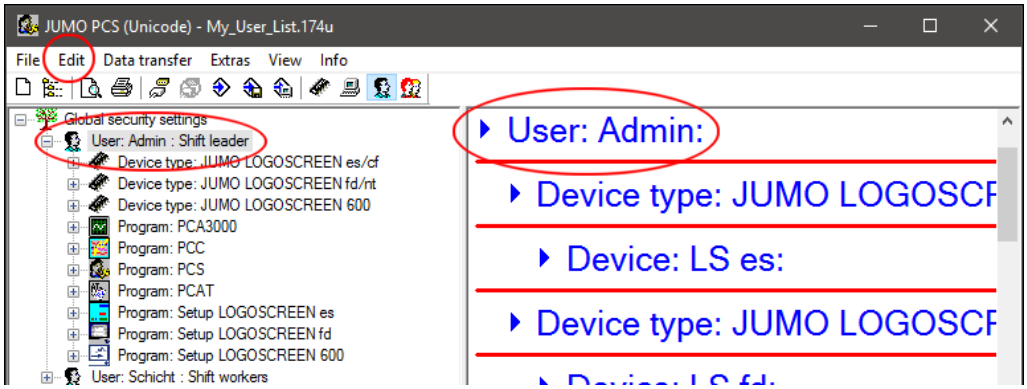
7.4.3 New user

Create new user

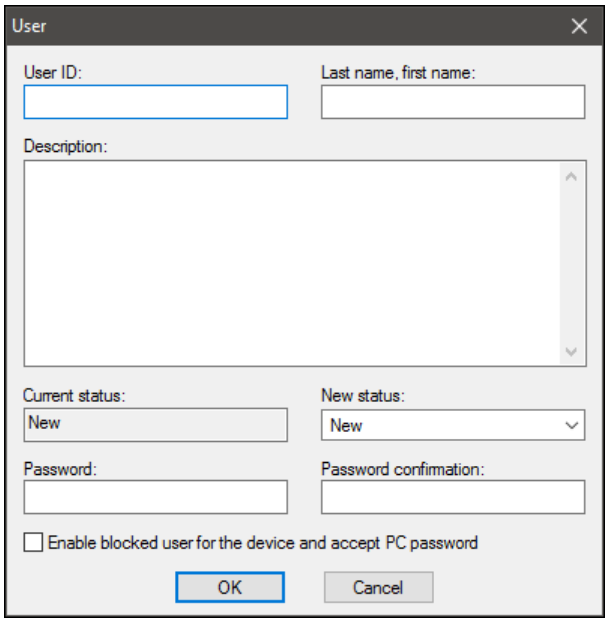
If a new user is created, this user can no longer be removed from the user list!

✱ Select a "user" in the navigation tree and invoke the **New user** command using the right mouse button.

Alternatively, select a "user" in the dialog window and invoke the **New user** command using the right mouse button or invoke the **EDIT > NEW USER** command via the menu bar.



The following dialog window opens:



User ID The user ID **must** be assigned when creating a new user.

Last name, first name The last name and first name or a designation **can** be assigned when creating a new user.

New status ⇨ "New status", page 68

Password/password confirmation A password **can** be created here for the new user.

⇨ "Define administrator", page 26

The user newly created by the administrator muss log on to the device/program again and is prompted to change their password.

⇨ "Options for program start", page 28

✱ Complete the entries using the OK button.

7.4.4 Device/computer group assignment: edit

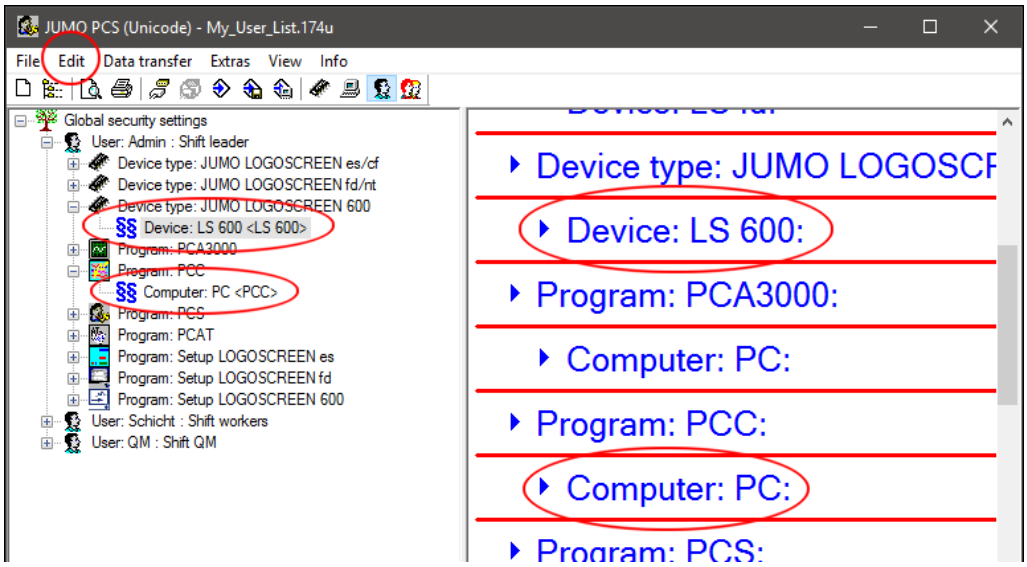
Groups available by default or newly created groups (user rights) can be assigned to or removed from each device/computer.

Any change to the device/program rights in this view may also affect previously assigned user rights for this device or program in the **View according to users** (Page 40) or the **View according to PCs** (Page 54).

Allocate groups (user rights)

* Select the corresponding "device" or "computer" in the navigation tree and invoke the **Device/computer group assignment: edit** command using the right mouse button.

Alternatively, select the corresponding "device" or "computer" in the dialog window and invoke the **Device/computer group assignment: edit** command using the right mouse button or invoke the **EDIT > DEVICE/COMPUTER GROUP ASSIGNMENT: EDIT** command via the menu bar.



The further course of action is the same as the description in the **View according to devices**.

⇨ Chapter 7.2.4 "User group assignment: edit"

7 Edit user lists

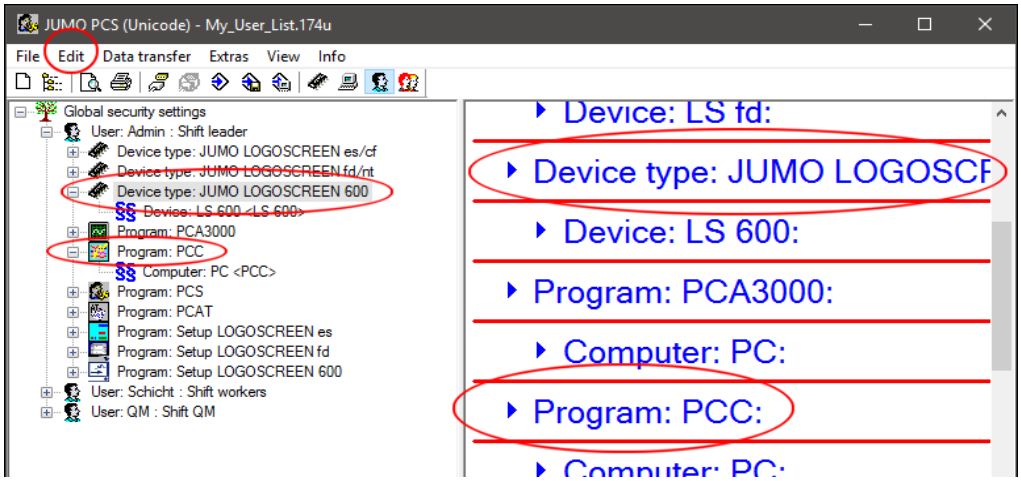
7.4.5 New device/program rights

New device/program rights (user rights) for all available device types or programs can be assigned to each user.

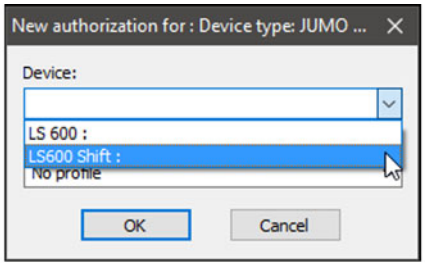
Assign new device/program rights

* Select the corresponding "device type" or "program" in the navigation tree and invoke the **New device/program rights** command using the right mouse button.

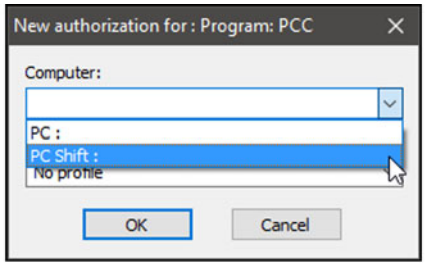
Alternatively, select the corresponding "device type" or "program" in the dialog window and invoke the **New device/program rights** command using the right mouse button or invoke the **EDIT > NEW DEVICE/PROGRAM RIGHTS** command via the menu bar.



* Select the device or computer in the following dialog and confirm using the button. OK



New device rights



New program rights

The further course of action is the same as the description in the **View according to devices**.

⇨ Chapter 7.2.4 "User group assignment: edit"

7.4.6 Remove

Device type/ program authorizations: remove

Removes all the device or program rights assigned to the user and the associated user rights (groups) from the list.

* Select the corresponding "device type" or "program" in the navigation tree and invoke the **Device type/program authorizations: remove** command using the right mouse button.

Device/computer group assignment: remove

Removes the selected device or program right and the associated user rights (groups) from the list.

* Select the corresponding device or program right in the navigation tree and invoke the **Device/computer group assignment: remove** command using the right mouse button.

The "Global security settings", "User", "Device type" and "Program" entries cannot be removed.

7.4.7 General functions in this view

The following functions can be accessed in this view using the right mouse button (context menu) in all entries of the navigation tree and the dialog window.

Expand node

⇨ "Expand/collapse node", page 34

Collapse node

⇨ "Expand/collapse node", page 34

Maximize/minimize device type/computer/ program

⇨ "Maximize/minimize", page 34

Copy device type/computer/ program to clipboard

The information listed in the dialog window about the device type/computer/ program is copied to the clipboard and can be added, e.g. in a text-processing program.

Copy everything to clipboard

Copies all information in the dialog window concerning general safety provisions, device type, computer and program to the clipboard.

Print

* "Print", page 119

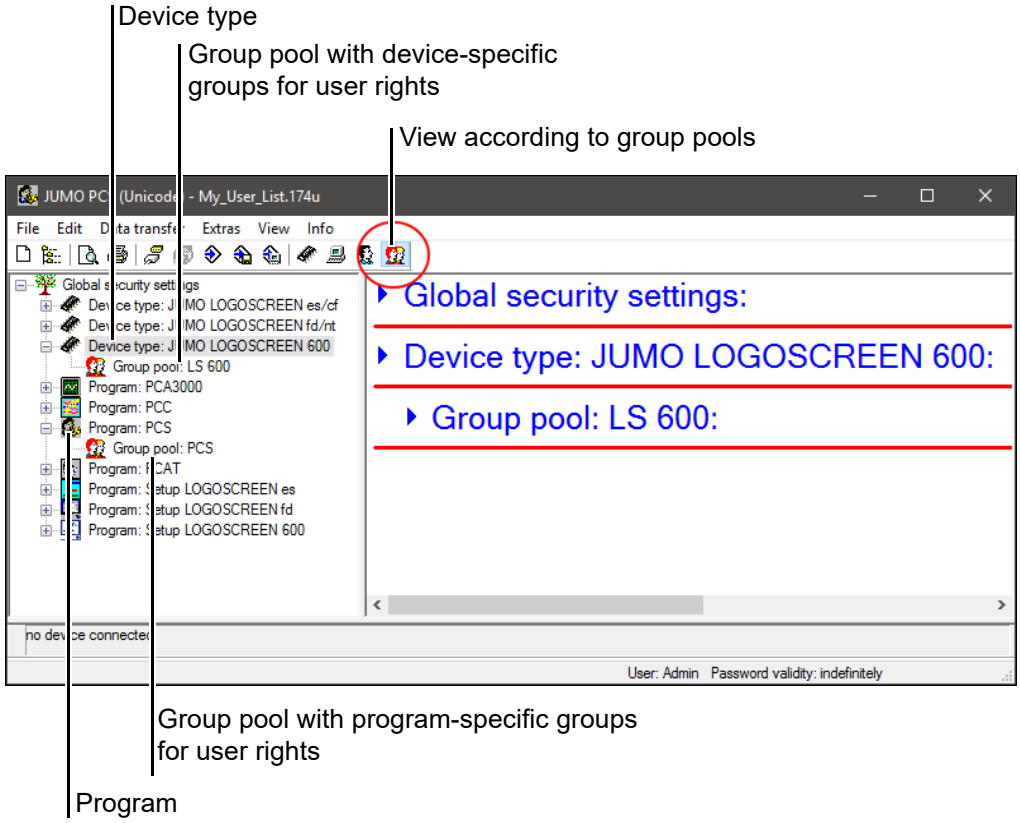
7 Edit user lists

7.5 View according to group pools

This view shows the group pools (available by default) for FDA-compliant devices and programs.

Open view

* Open the **VIEW > VIEW ACCORDING TO GROUP POOLS** menu or press the corresponding button in the toolbar.

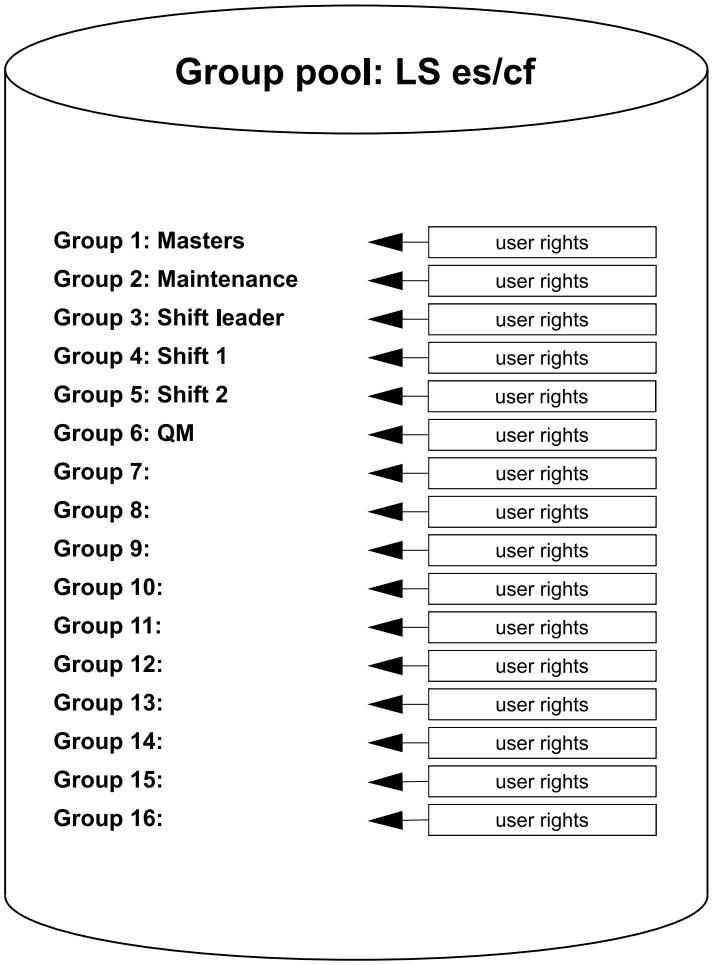


Device type/ program

All FDA-compliant "device types" and "programs" are assigned by default to the created user (administrator).

What are group pools?

Example: Group pool JUMO LOGOSCREEN es/cf (diagram)



A group pool is already assigned to each FDA-compliant device/program by default (e.g. JUMO LOGOSCREEN 600 or JUMO PCA3000).

Each device-specific and program-specific group pool manages 16 groups with user rights.

The group pools assigned to the devices and programs provide a preselection of groups with user rights in the views **according to devices** (Page 40) and **according to PCs** (Page 54) and thus simplify the assignment of rights to users.

Groups

Groups describe the role or task of users of the device/program (e.g. a shift leader). Device-specific and program-specific groups are already predefined by default (e.g. masters, maintenance).

User rights in groups

Device-specific and program-specific user rights are allocated to groups. Device-specific and program-specific user rights are already assigned to predefined groups by default (e.g. masters, maintenance).

7.5.1 Functions in the view according to group pools

The following functions can be executed in this view:

- **Edit global security settings**

⇨ Chapter 5.6.1 "Edit global security settings"

- **Edit group pools available by default**

⇨ Chapter 7.5.2 "Edit group pool"

- **Edit user rights**

⇨ "Edit user rights", page 79

- **Create new group pools**

⇨ Chapter 7.5.3 "New group pool"

- **Remove group pools**

⇨ Chapter 7.5.4 "Remove"

- **General functions in this view**

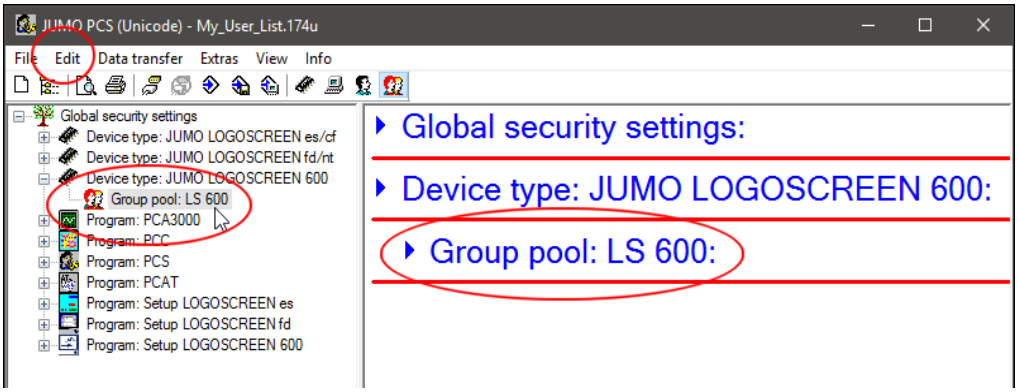
⇨ Chapter 7.5.5 "General functions in this view"

7.5.2 Edit group pool

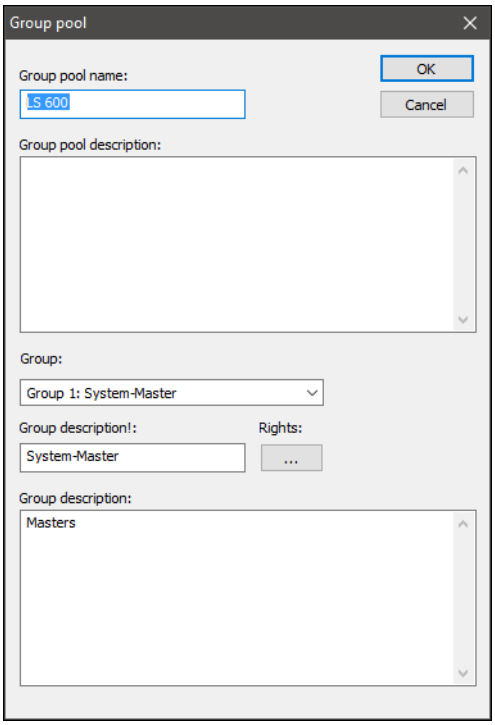
Existing or newly created group pools for FDA-compliant device types and programs can be subsequently processed by default.

✱ Select the corresponding "group pool" in the navigation tree and invoke the **Group pool: edit** command using the right mouse button.

Alternatively, select the corresponding "group pool" in the navigation tree and invoke the **Group pool: edit** command using the right mouse button or invoke the **EDIT > GROUP POOL: EDIT** command via the menu bar.



The following dialog window opens:

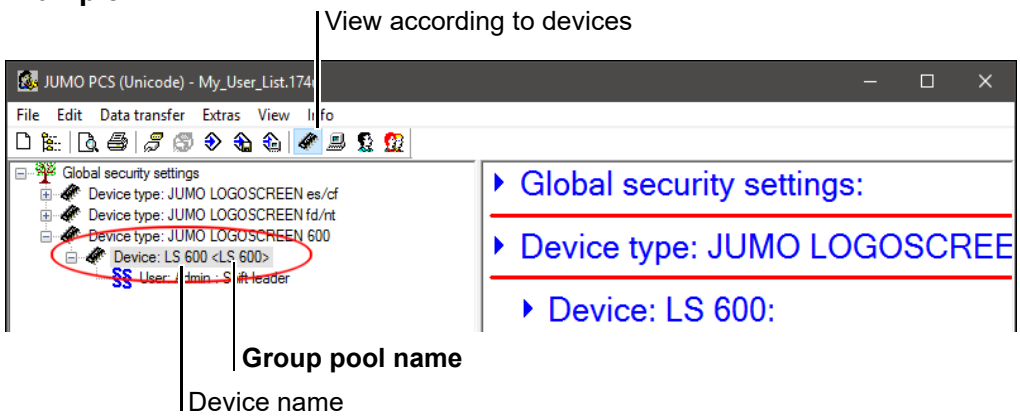


Group pool name

✱ Enter the new group pool name.

The **<Name>** of the group pool is displayed in the remaining views.

Example:



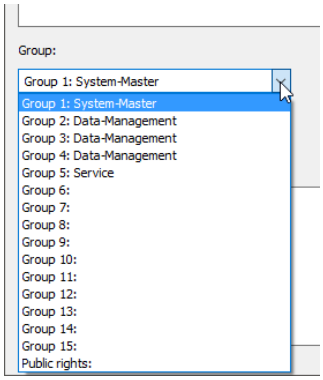
Group pool description

Add a description of the group pool if necessary, e.g. the device location or the program name.

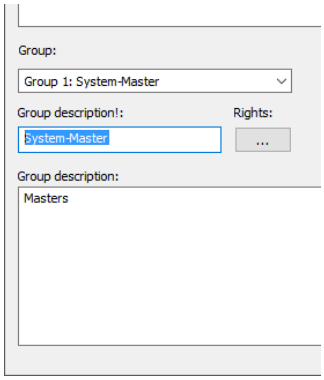
Group/group designation/ group description

Example: Edit device-specific and program-specific group

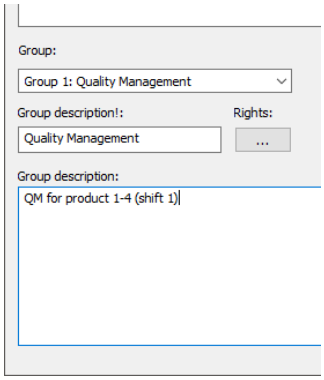
✱ Select group



✱ Change designation

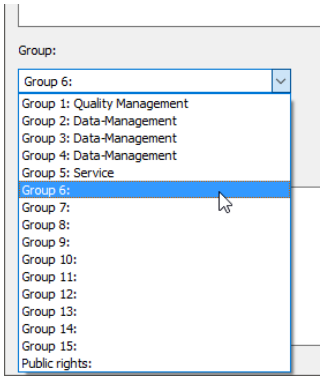


✱ Change description

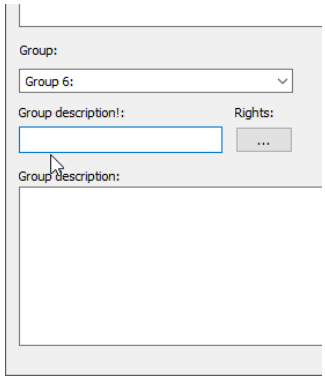


Example: Edit freely assignable group

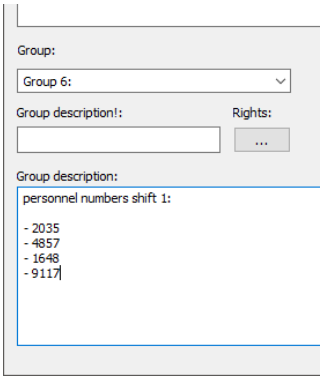
✱ Select group



✱ Enter designation



✱ Change description



Rights

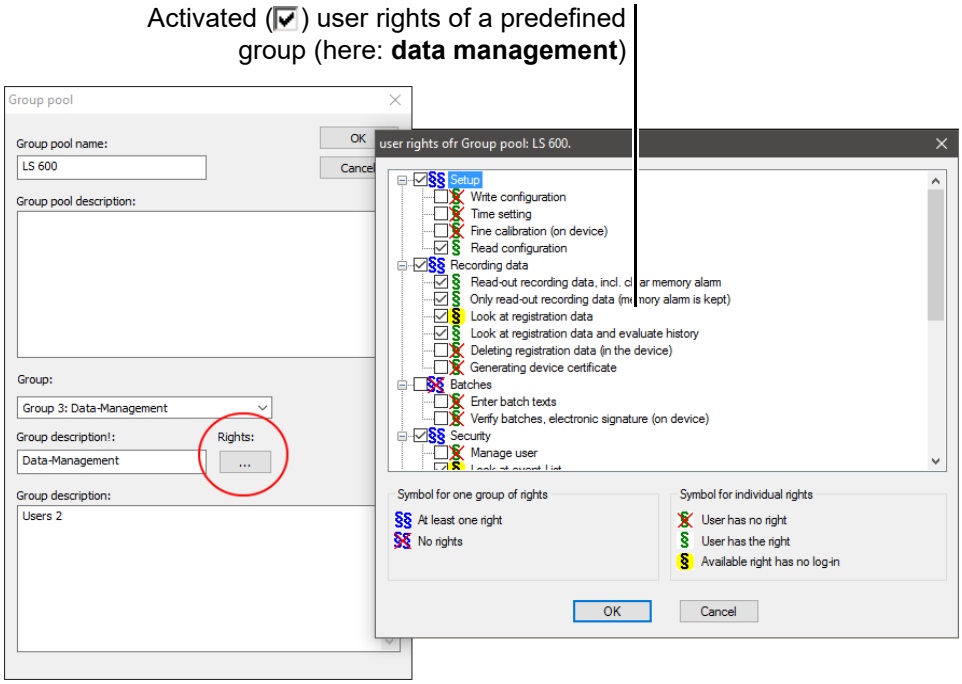
Device-specific and program-specific user rights are already allocated to device-specific and program-specific groups (e.g. master or maintenance).

Edit user rights

✱ Click the **RIGHT** button.

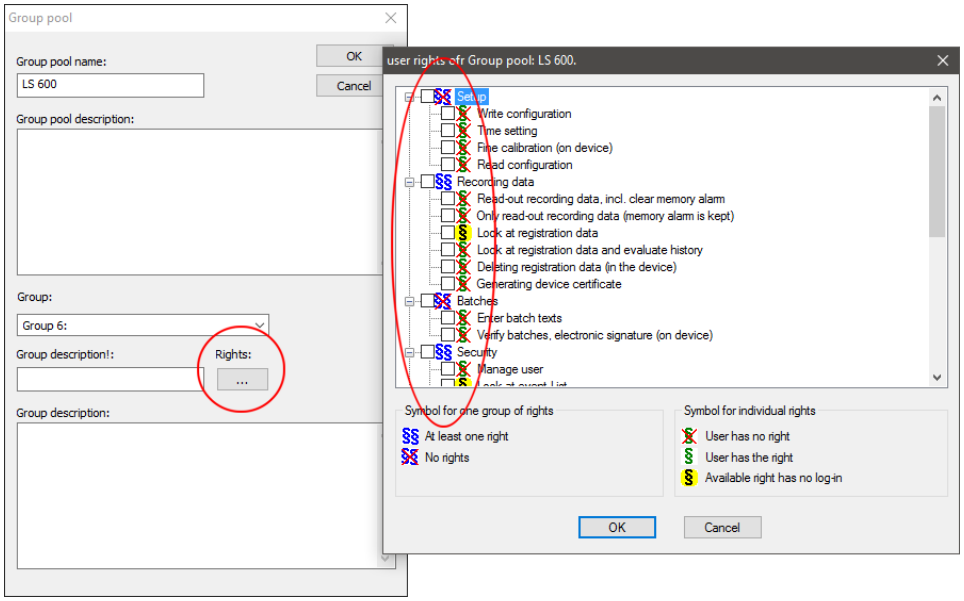
The **User rights for group pool...** dialog window opens.

Activated (☑) user rights of a predefined group (here: **data management**)



✱ Expand or limit the device-specific and program-specific user rights by enabling (☑) or disabling (☐) and confirm using the OK button.

No user rights are assigned to freely assignable groups.



✱ Expand or limit the user rights by enabling (☑) or disabling (☐) and confirm using the OK button.

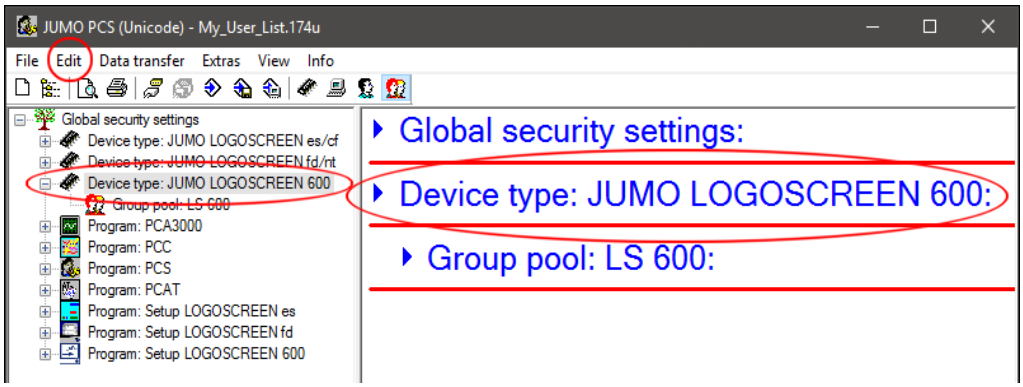
7.5.3 New group pool

New group pools with device-specific and program-specific user rights can be assigned to each device type/program.

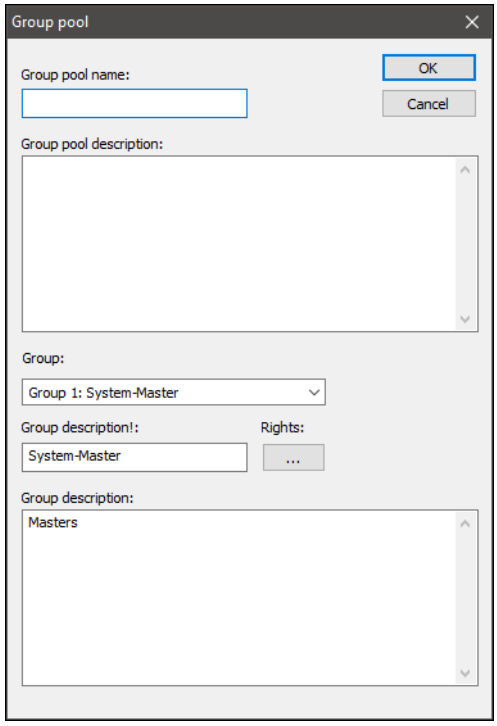
Create new group pool

* Select the corresponding "device type" or "program" in the navigation tree and invoke the **New group pool** command using the right mouse button.

Alternatively, select the corresponding "device type" or "program" in the dialog window and invoke the **New group pool** command using the right mouse button or invoke the **EDIT > NEW GROUP POOL** command via the menu bar.



The following dialog window opens:



The further course of action for creating new group pools is the same as in .Chapter 7.5.2 "Edit group pool"

7.5.4 Remove

Group pool: remove

Removes the selected group pool, incl. all device-specific and program-specific user rights in the group from the list.

* Select the corresponding "group pool" in the navigation tree and invoke the **Group pool: remove** command using the right mouse button.

Device type/ program authorizations: remove

Removes all the group pools assigned to the device type/program and the associated user rights in the groups from the list.

* Select the corresponding "device type" or "program" in the navigation tree and invoke the **Device type/program authorizations: remove** command using the right mouse button.

The "Global security settings", "Device type" and "Program" entries cannot be removed.

7.5.5 General functions in this view

The following functions can be accessed in this view using the right mouse button (context menu) in all entries of the navigation tree and the dialog window.

Expand node

⇨ "Expand/collapse node", page 34

Collapse node

⇨ "Expand/collapse node", page 34

Maximize/minimize device type/program/ group pool

⇨ "Maximize/minimize", page 34

Copy device type/program/ group pool to clipboard

The information listed in the dialog window about the device type/program/ group pool is copied to the clipboard and can be added, e.g. in a text-processing program.

Copy everything to clipboard

Copies all information in the dialog window concerning general safety provisions, device type, program and group pool to the clipboard.

Print

⇨ "Print", page 119

7 Edit user lists

7.6 View according to profiles

This view is only available if a user list was opened from databases that contain profiles.

These user lists can still be edited and processed.

Profiles/profile rights can also be converted into groups within group pools.

⇨ Chapter 7.6.7 "Convert user list"

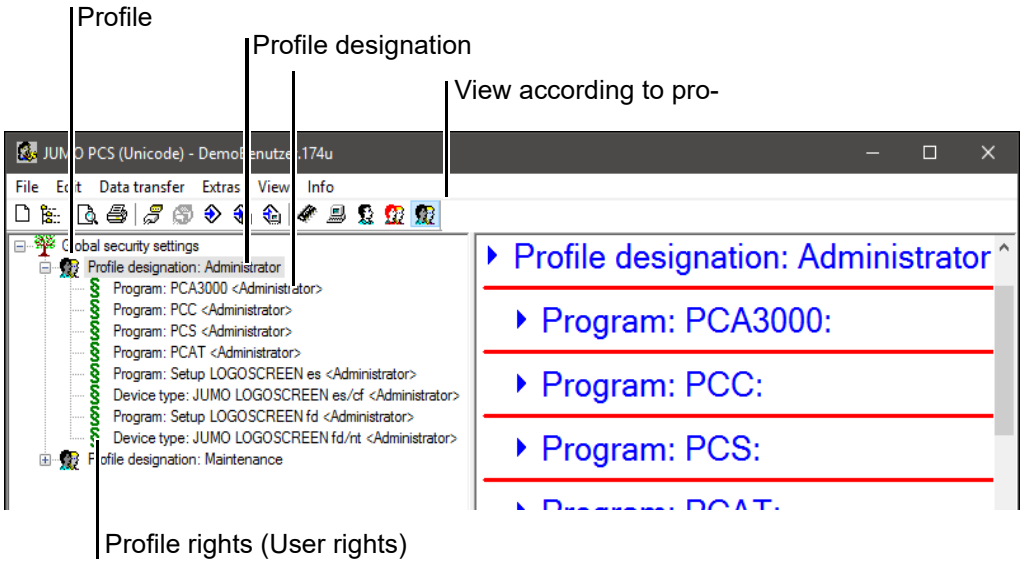
A profile service to preallocate user rights when creating new user rights for device, programs or users.

The preallocation of user rights in profiles can be subsequently edited in the views according to devices, PCs and users.

⇨ Chapter 7.6.6 "Apply profile rights in views"

Open view

✱ Open the **VIEW > VIEW ACCORDING TO PROFILES** menu or press the corresponding button in the toolbar.



Profile

Created profile for a user. New profile rights (user rights) for programs and devices can be allocated to the profile.

Profile designation

The profile designation can be specified when creating a new profile and identifies the profile rights created in this profile.

Profile rights

Device-specific and program-specific user rights are allocated to profile rights. The user rights can be edited and used as templates for user rights in the views according to devices ( ) and according to PCs.

7.6.1 Functions in the view according to profiles

The following functions can be executed in this view:

- **Edit global security settings**

⇨ Chapter 5.6.1 "Edit global security settings"

- **Edit available profiles**

⇨ Chapter 7.6.2 "Edit profile"

- **Create new profiles**

⇨ Chapter 7.6.3 "New profile"

- **Edit available profile rights (user rights)**

⇨ Chapter 7.6.4 "Edit user rights"

- Generate new profile rights (user rights)

⇨ Chapter 7.6.5 "New profile rights (user rights)"

- **Apply/edit profile rights in all views**

⇨ Chapter 7.6.6 "Apply profile rights in views"

- **Generate group pools from available profile rights**

⇨ Chapter 7.6.7 "Convert user list"

- **Remove profiles and profile rights**

⇨ Chapter 7.6.8 "Remove"

- **General functions in this view**

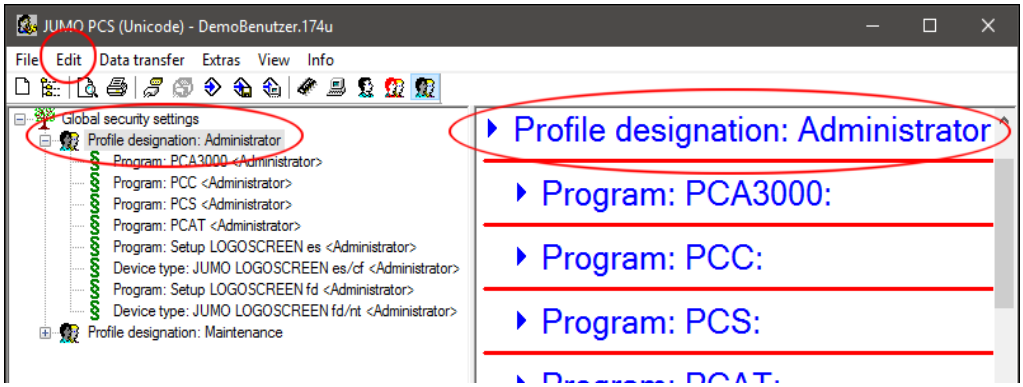
⇨ Chapter 7.6.9 "General functions in this view"

7.6.2 Edit profile

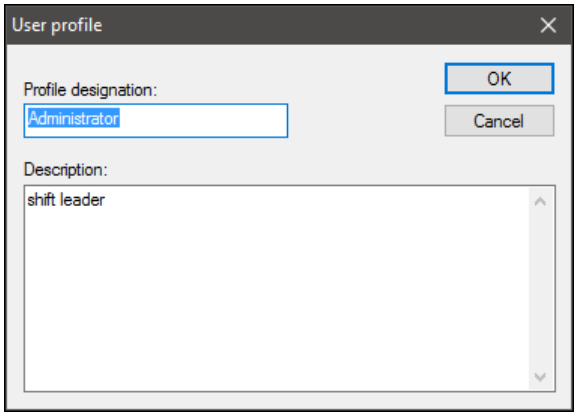
Edit profile designation

* Select the corresponding "profile" in the navigation tree and invoke the **Profile designation: edit** command using the right mouse button.

Alternatively, select the corresponding "profile" in the dialog window and invoke the **Profile designation: edit** command using the right mouse button or invoke the **EDIT > PROFILE DESIGNATION: EDIT** command via the menu bar.



The following dialog window opens:



Profile designation

The profile designation can be altered. A profile designation **must** be entered.

Description

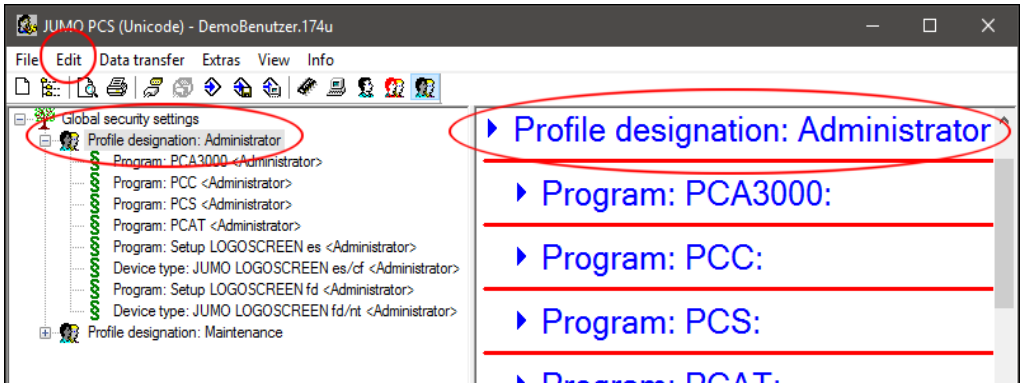
The description of the profile **can** be supplemented, altered or deleted.

7.6.3 New profile

Create new profile

Select the corresponding "profile" in the navigation tree and invoke the **New profile** command using the right mouse button.

Alternatively, select the corresponding "profile" in the dialog window and invoke the **New profile** command using the right mouse button or invoke the **Edit > New profile** command via the menu bar.



The further course of action for creating a new device is the same as in Chapter 7.2.2 "Edit device".

Profile rights (user rights) for programs and devices can now be assigned to the new profile.

⇨ Chapter 7.6.5 "New profile rights (user rights)"

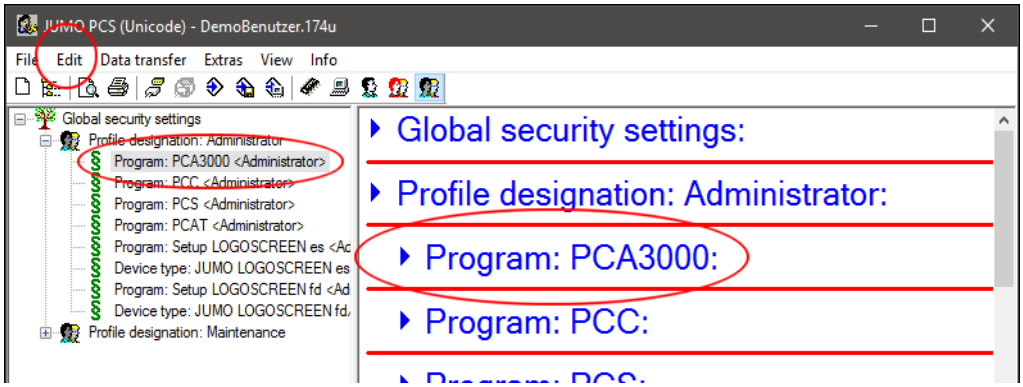
7 Edit user lists

7.6.4 Edit user rights

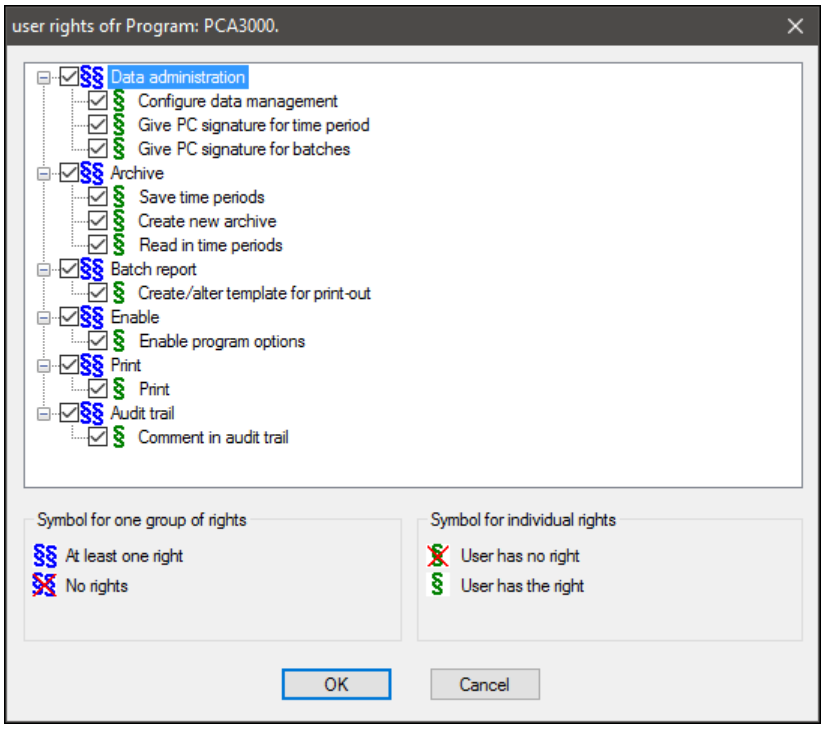
Edit program/ device user rights

Select the corresponding "device" or "program" in the navigation tree and invoke the **Edit device/program user rights** command using the right mouse button.

Alternatively, select the corresponding "device" or "program" in the dialog window and invoke the **Device/program user rights: edit** command using the right mouse button or invoke the **EDIT > DEVICE/PROGRAM USER RIGHTS** command via the menu bar.



The following dialog window opens:



Expand or limit the device-specific and program-specific user rights by enabling (☑) or disabling (☐) and confirm using the OK button.

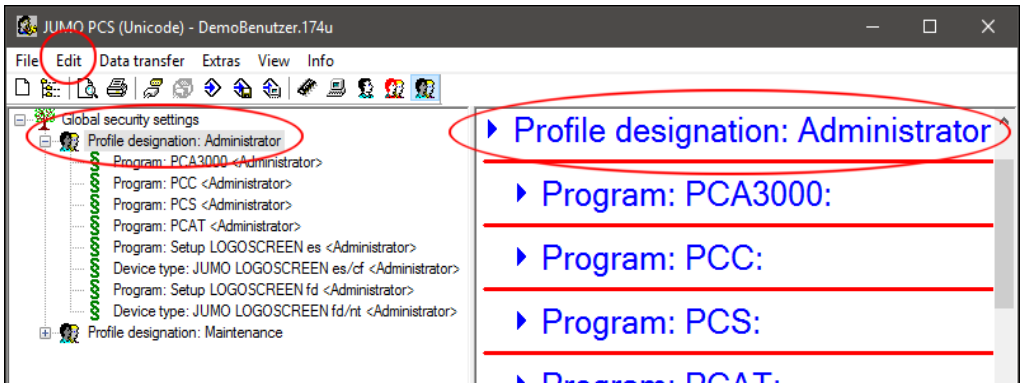
7.6.5 New profile rights (user rights)

New device-specific and program-specific profile rights (user rights) can be created in a new profile.

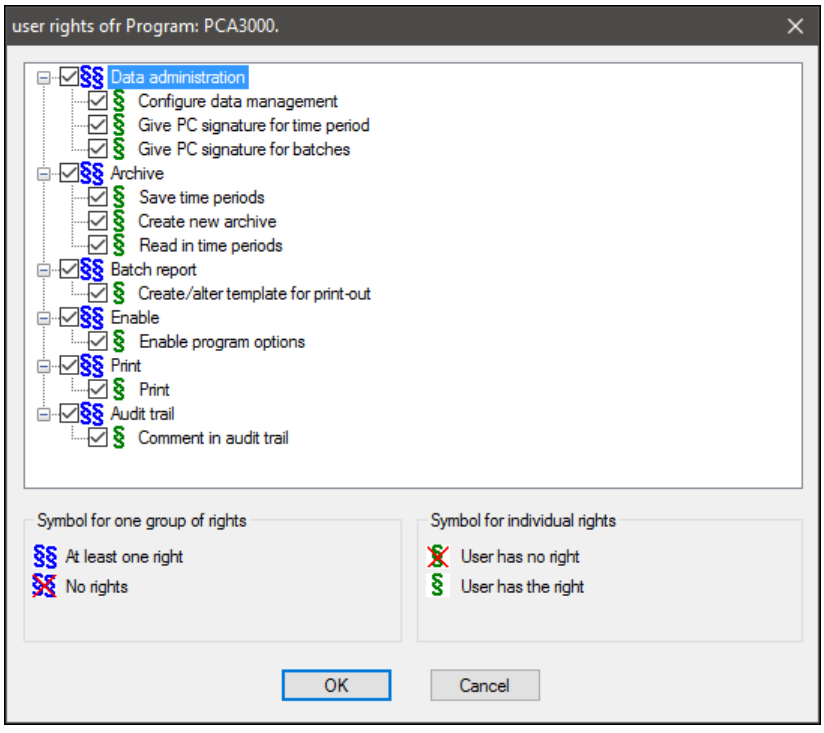
Create profile rights for programs/device

* Select the corresponding "profile" in the navigation tree and invoke the **New profile rights** command using the right mouse button.

Alternatively, select the corresponding "profile" in the dialog window and invoke the **New profile rights** command using the right mouse button or invoke the **EDIT > NEW PROFILE RIGHTS** command via the menu bar.



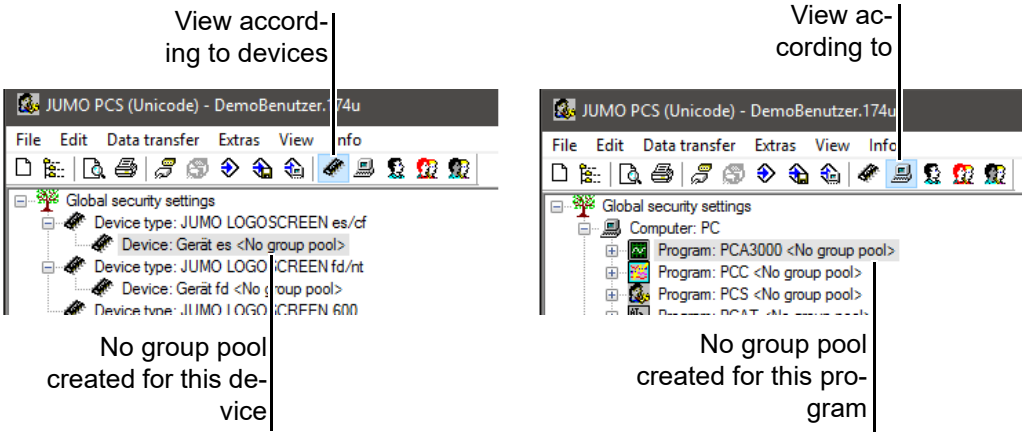
The following dialog window opens:



Expand or limit the device-specific and program-specific user rights by enabling (☑) or disabling (☐) and confirm using the OK button.

7.6.6 Apply profile rights in views

Device-specific and program-specific profile rights (user rights) that were generated for a profile can be used as a template in the views according to devices , according to PCs and according to users if no group pool has been created or assigned for the device or program.



The JUMO LOGOSCREEN 600, 601 and 700 devices only work with user rights from group pools.

If user rights need to be created for the JUMO LOGOSCREEN 600, 601 or 700 devices in the user lists without group pools, a group pool needs to be created first.

⇨ "Create group pool", page 91

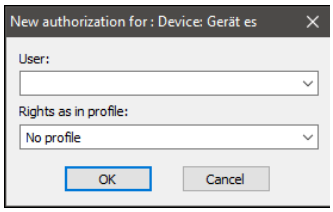
Create new user rights in the views

* Select view according to devices , according to PCs or according to users .
* Select the corresponding "device" or "program" in the navigation tree of the selected view and invoke the **New user rights** command using the right mouse button.

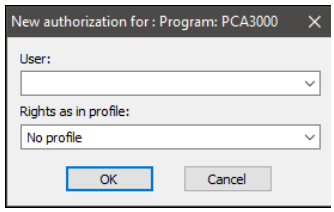
Alternatively, select the corresponding "device" or "program" in the dialog window of the selected view and invoke the **NEW USER RIGHTS** command using the right mouse button or invoke the **EDIT > NEW USER RIGHTS** command via the menu bar.

The following dialog window open depending on the selected view:

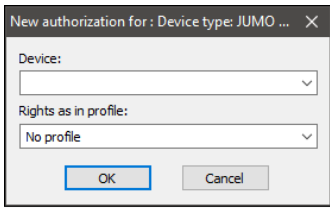
View according to devices:

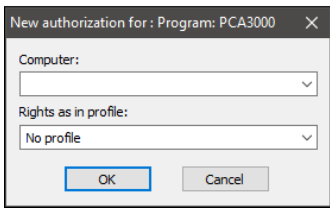


View according to PCs:



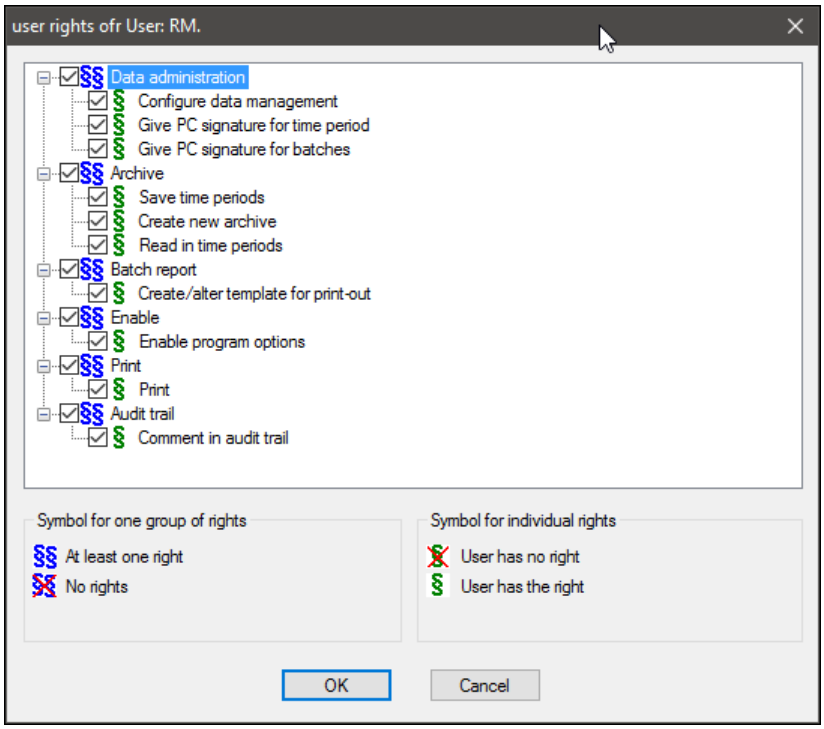
View according to users:





* Select user, device or computer from the drop-down menu.
* Select profile from the drop-down menu and confirm using the OK button.

The following dialog window opens depending on the selection made:



Device-specific and program-specific profile rights (user rights) that were generated for the selected profile, and can be used as a template here and subsequently edited are depicted.

* Expand or limit the device-specific and program-specific user rights by enabling (☑) or disabling (☐) and confirm using the OK button.

New user rights are created for the selected device/program.

7 Edit user lists

7.6.7 Convert user list

If new devices or programs are created in user lists containing profiles, a group pool first needs to be created for the corresponding device or program.

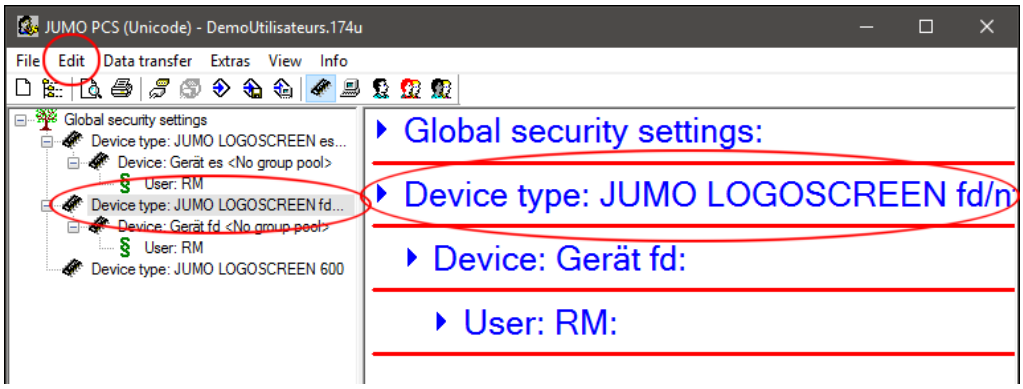
If a new group pool is created, the existing user list needs to be converted.

In this step, the user rights coming from profiles become user rights in groups from a group pool.

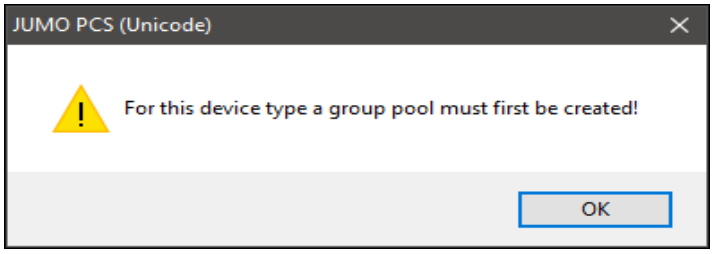
Example: Creating a new device

* Switch to the View according to devices .
* Select the corresponding "device type" in the navigation tree and invoke the **New device** command using the right mouse button.

Alternatively, select the corresponding "device type" in the dialog window and invoke the **New device** command using the right mouse button or invoke the **EDIT > NEW DEVICE** command via the menu bar.

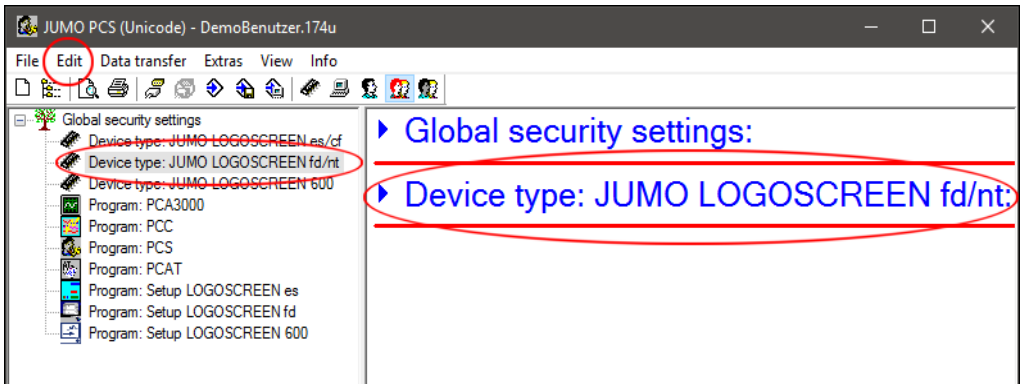


The following dialog window opens:

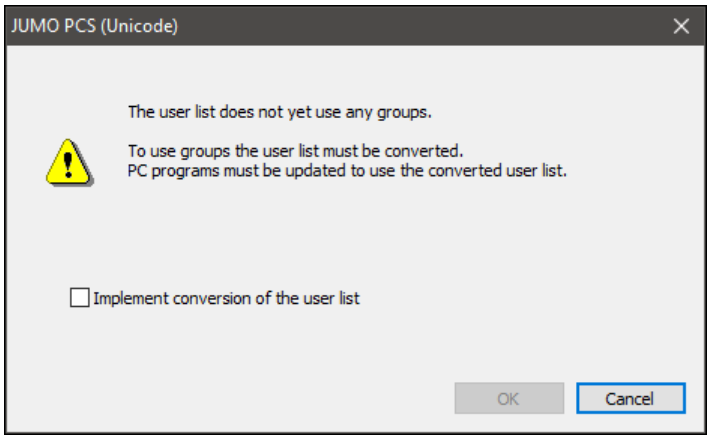


Create group pool

* Switch to the view according to group pools .
* Select the corresponding "device type" in the navigation tree and invoke the **New group pool** command using the right mouse button.
* Alternatively, select the corresponding "device type" in the dialog window and invoke the **New group pool** command using the right mouse button or invoke the **EDIT > NEW GROUP POOL** command via the menu bar.



The following dialog window opens:



Convert user list

The current user list with profile rights must be converted.

The user rights for device, programs and users coming from the profile rights remain unchanged and can continue to be edited.

If new devices and PCs are created after the conversion, it is only possible to create device-specific and program-specific user rights for the new devices and PCs via group pools.

⇨ Chapter 7.5 "View according to group pools"

* Activate the checkbox (☑) and confirm using the OK button.

The user list is converted.

Convert user lists - example 1

Initial situation:

A user list contains four profiles. Three profiles include user rights for the JUMO LOGOSCREEN fd/nt device type. The "Layer 01" profile does not include any user rights for this device type.

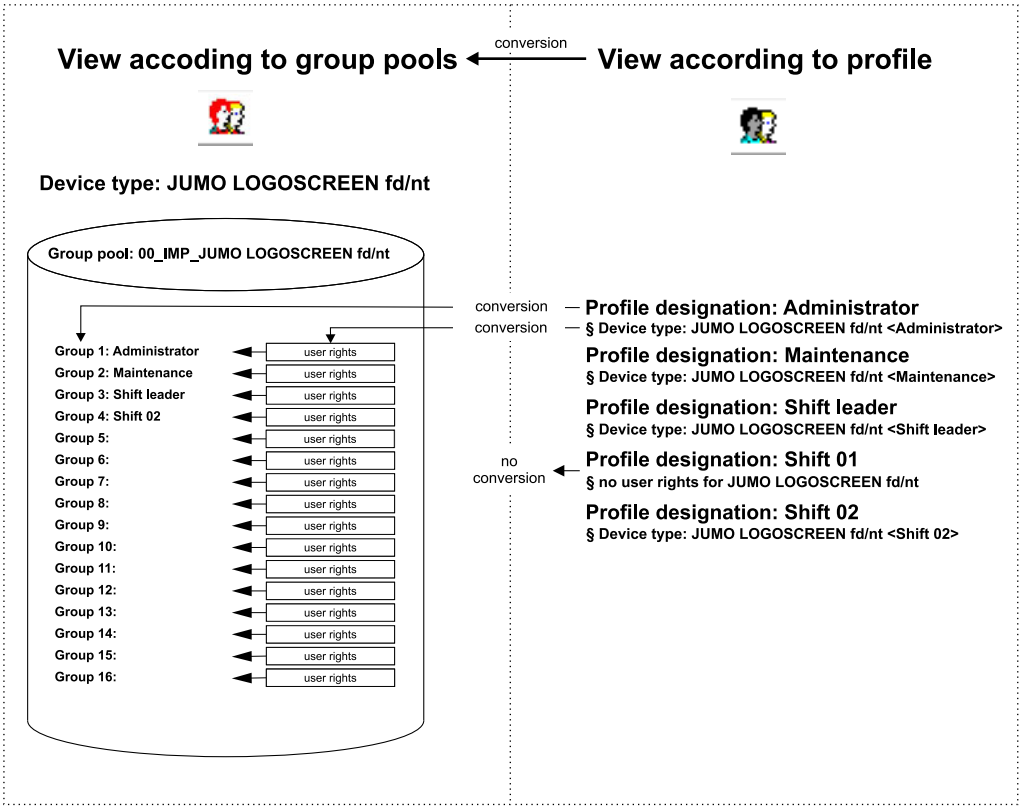
Conversion process:

- The "00_IMP_JUMO LOGOSCREEN fd/nt" group pool comes from the JUMO LOGOSCREEN fd/nt device type.
- Groups come from all profiles **with** user rights for the JUMO LOGOSCREEN fd/nt device, e.g. **profile designation: administrator** becomes **group 1: administrator**.

Profiles that do not include **any** user rights for this device are converted into a group in the group pool created (see: **profile designation: layer 02**).

- The user rights for the JUMO LOGOSCREEN fd/nt device from the profiles are stored in the groups of the group pools created. Example: JUMO LOGOSCREEN fd/nt profile rights for **profile designation: administrator** become **group 1: administrator** in the "00_IMP_JUMO LOGOSCREEN fd/nt" group pool.

Schematic view of the conversion process:



Convert user lists - example 2

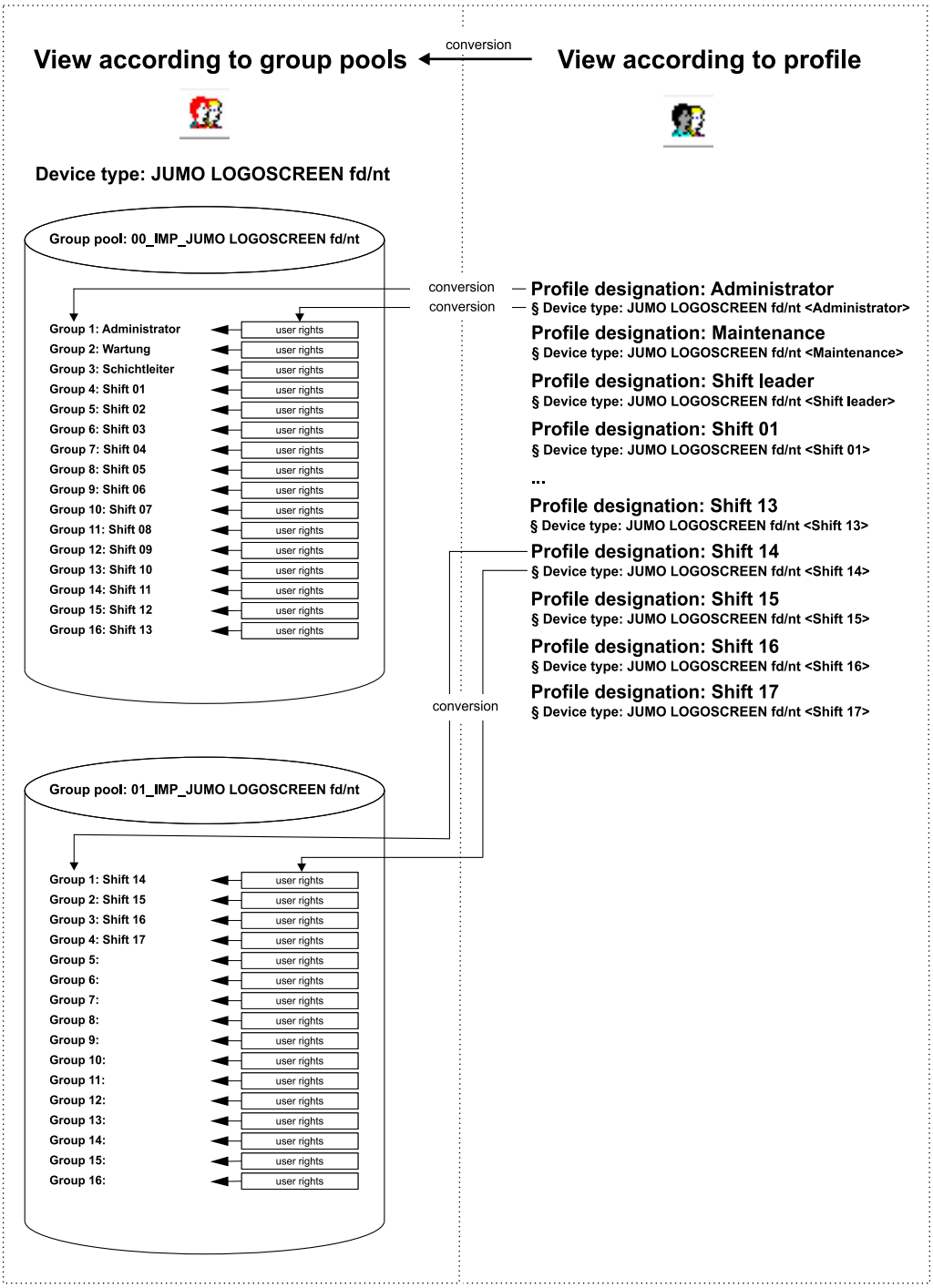
Initial situation:

A user list contains 20 profiles. All profiles include user rights for the JUMO LOGOSCREEN fd/nt device type.

Conversion process:

- see "Convert user lists - example 1", page 92
- If there are more than 16 profiles with user rights for a device type/program, a second group pool is formed for profiles 17 to 32, etc.

Schematic view of the conversion process:



7.6.8 Remove

Profile designation: remove

Removes the selected profile, incl. all device-specific and program-specific user rights (profile rights) from the list.

* Select the corresponding "profile designation" in the navigation tree and invoke the **Profile designation: remove** command using the right mouse button.

Device type/ program user rights: remove

Removes all the user rights (profile rights) assigned to the device type/program from the list.

* Select the corresponding "device type" or "program" in the navigation tree and invoke the **Device type/program user rights: remove** command using the right mouse button.

The "Global security settings" entry cannot be removed.

7.6.9 General functions in this view

The following functions can be accessed in this view using the right mouse button (context menu) in all entries of the navigation tree and the dialog window.

Expand node

⇨ "Expand/collapse node", page 34

Collapse node

⇨ "Expand/collapse node", page 34

Maximize/minimize profile designation/ user rights

⇨ "Maximize/minimize", page 34

Copy profile designation/ user rights to clipboard

The information listed in the dialog window about the profile designation/user rights is copied to the clipboard and can be added, e.g. in a text-processing program.

Copy everything to clipboard

Copies all information in the dialog window concerning general safety provisions, device type, device, users and profiles to the clipboard.

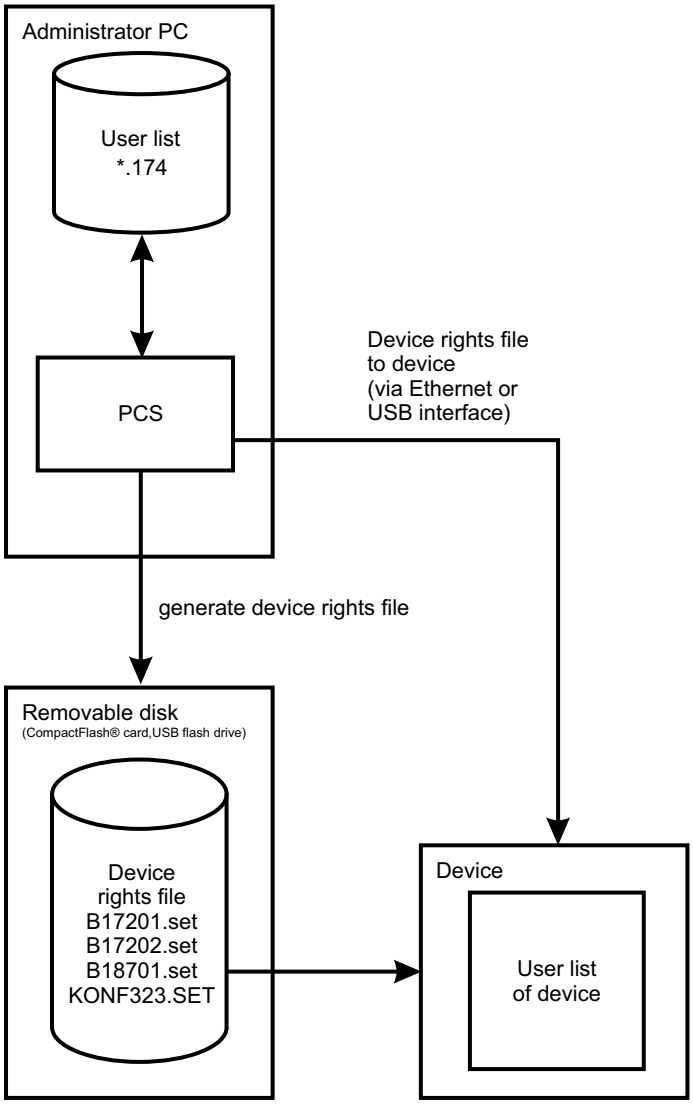
Print

"Print", page 119

User lists can be transmitted as device rights files from PCS to the device in the following ways:

Direct Data transfer via an Ethernet or serial interface to the device ("Transfer via an interface", page 96)

Indirect Data transfer to the device via a removable disc ("Transfer via removable disc", page 106)



The direct transfer of a device rights file via an interface is performed with the "Device rights file for the device", page 104 function.

The indirect transfer of a device rights file via a removable disc is performed with the "Generate device rights file", page 106 function.

8 Data transfer to the device

8.1 Transfer via an interface

8.1.1 Hardware requirements

Data can be transferred via one of the following interfaces:

Device	PCS via PC
Ethernet	Ethernet
USB device	USB host

Ethernet

A device or a PC can be connected to a network using commercially available network cables (RJ45 connector). Establish a direct connection between the device and PC using a crossover cable.

Only **one** PC program (client such as PCC, PCS or setup program) can access the device (server) via the Ethernet interface at any time.

USB device

A device or a PC can be connected to a network using commercially available USB cables with a maximum length of 3 m.

8.1.2 Connection settings wizard

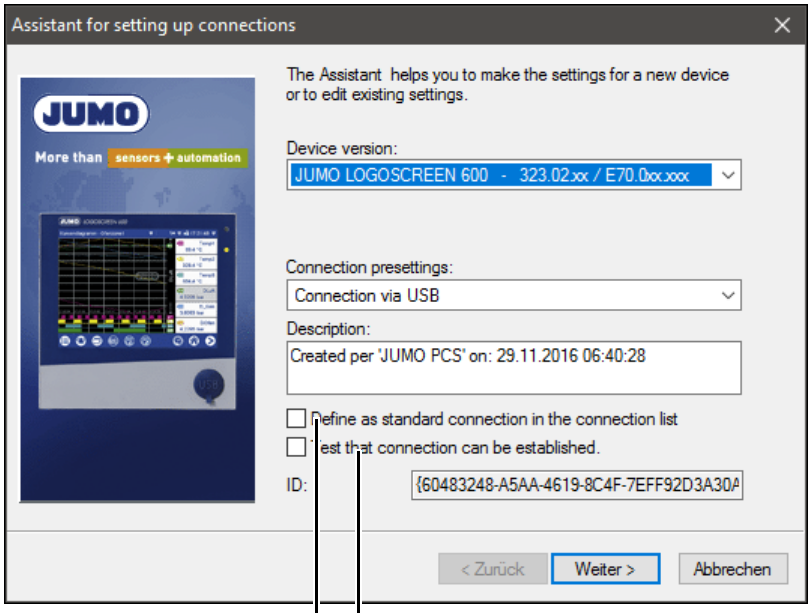
If data needs to be exchanged between PCS via a PC and a device, connection settings also need to be defined in addition to the hardware requirements ("Hardware requirements", page 96).

Establish connection

✱ Establish a connection to the device via **DATA TRANSFER > ESTABLISH CONNECTION** in the menu bar or by clicking the  symbol in the toolbar.

Connection settings wizard

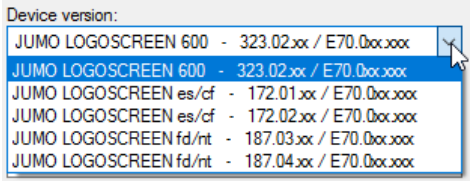
If this is the first time communication has been established with this device and the connection settings have not yet been defined, the **Connection settings wizard** starts.



If the option (☑) is activated, a test is performed following entry into the device connection list to see whether a connection can be established to the selected device via the selected interface.

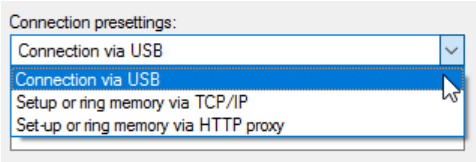
If activated (☑), a standard connection is automatically accessed. Other connections need to be established via the device connection list.

✱ Select the device version from the drop-down menu:



Default connection settings

Select the default connection settings from the drop-down menu:



* Activate the additional options where necessary (☑).
* Confirm the entries using the Next > key.

Do not log in

By default, the setup program is configured so that the logged in user is automatically logged in to a device found (with their name and password) and can thus communicate with the device if the necessary rights are activated for the user in the device user lists on the device.

* Activate the (☑) option if the user does not want to log on.

If the user is not logged in, the device's standard rights are used.

The functions on the device can be limited. The current device user list and the rights defined in it for the user are crucial.

Save ID and password

When the option is activated, the logon to the device occurs with the User ID and password to be entered, regardless of the current user in the setup program.

* Activate the additional options where necessary (☑).
* Confirm the entries using the Next > button.

Interface parameters

The next steps depend on the selected interface or connection type in the "Default connection settings", page 98.

TCP/IP PORT

The following parameters must be selected:

IP address/ HOST name	xxx.xxx.xxx.xxx (e.g.: 10.11.2.100 or Hall1-Furnace1)	Specify the PC IP address. By entering the name, the IP address can be determined by clicking the "Convert host name to IP address" button.
Port number, port name	80, 502 (LS es/cf)	Port via which communication occurs.

USB interface

The following parameters must be selected:

Connected devices	Select which device needs to be connected	Select available device.
Name (optional)	Activate test yes/no	Only connect devices with this name.
F-No. (optional)	Activate test yes/no	Only connect devices with this device number.
CPU (optional)	Activate test yes/no	Only connect devices with this CPU number.
Path (optional)	Activate test yes/no	Only connect devices to this USB path.

HTTP proxy

The following parameters must be selected:

IP address/ HOST name	xxx.xxx.xxx.xxx (e.g.: 10.11.2.100 or Hall1-Furnace1)	Specify the PC IP address. By entering the name, the IP address can be determined by clicking the "Convert host name to IP address" button.
Port number, port name	80, 502 (LS es/cf)	Port via which communication occurs.
Proxy	Proxy	
Proxy port	Proxy	

USB-TTL interface

The following parameters must be selected:

Connected converter		Select available converter
Transfer rate	9600, 19200, 38400	The transfer rate must correspond to the the transfer rate selected on the device.

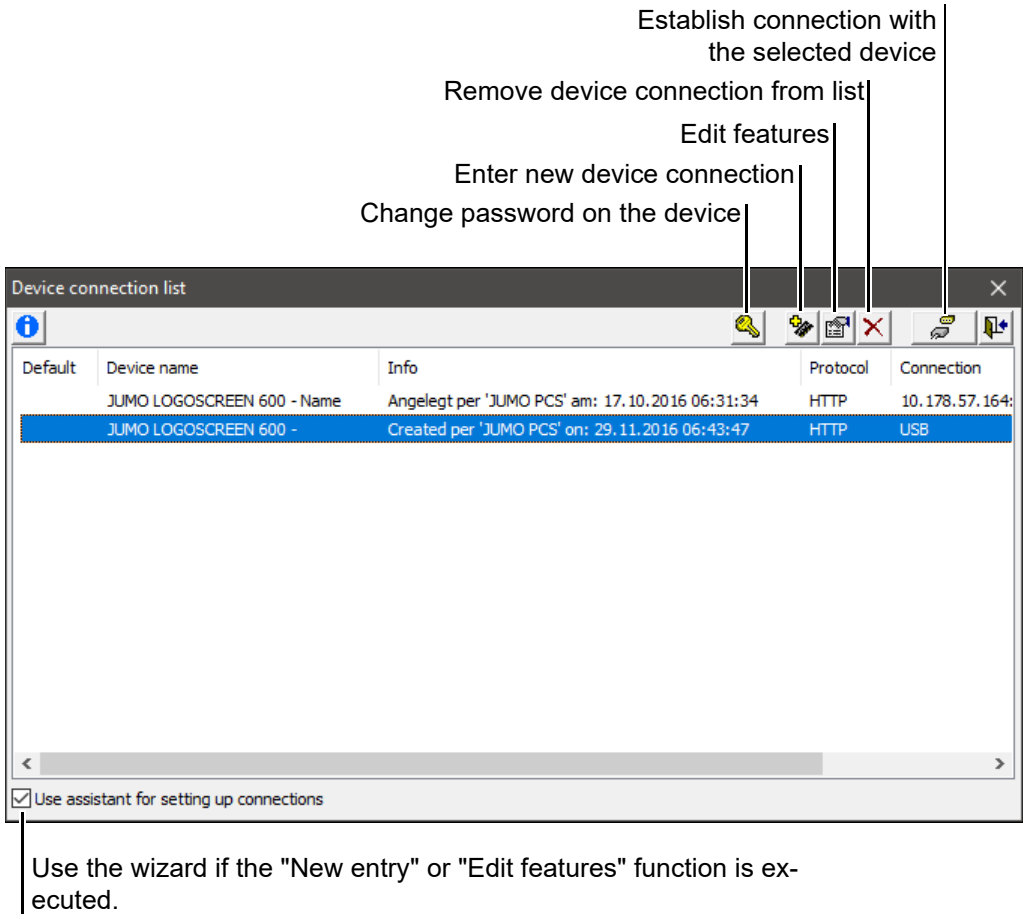
Device connection list

If all the settings have been made, the established connection between PCS and a device is entered into the device connection list.

⇨ Chapter 8.1.3 "Device connection list"

8.1.3 Device connection list

All defined connections between PCS and devices are displayed in a device connection list.



Change password on the device

Connects the selected list entry to the device and starts the **Change password on the device** dialog.

⇨ "Generate/change password", page 28

New entry

A new connection between PCS and a device can be established and the connection settings defined using this function.

If the "Connection settings wizard" option is activated (☑), the connection wizard starts. If not, the new connection must be established manually.

⇨ Chapter ChapterChapter 8.1.2 "Connection settings wizard", on page 97

Edit features

The connection settings can be subsequently edited for the selected list entry (device).

Establish connection with the device

Establishes the connection between PCS and the selected list entry (device).

⇨ Chapter ChapterChapter 8.1.4 "Establish/terminate connection", on page 102

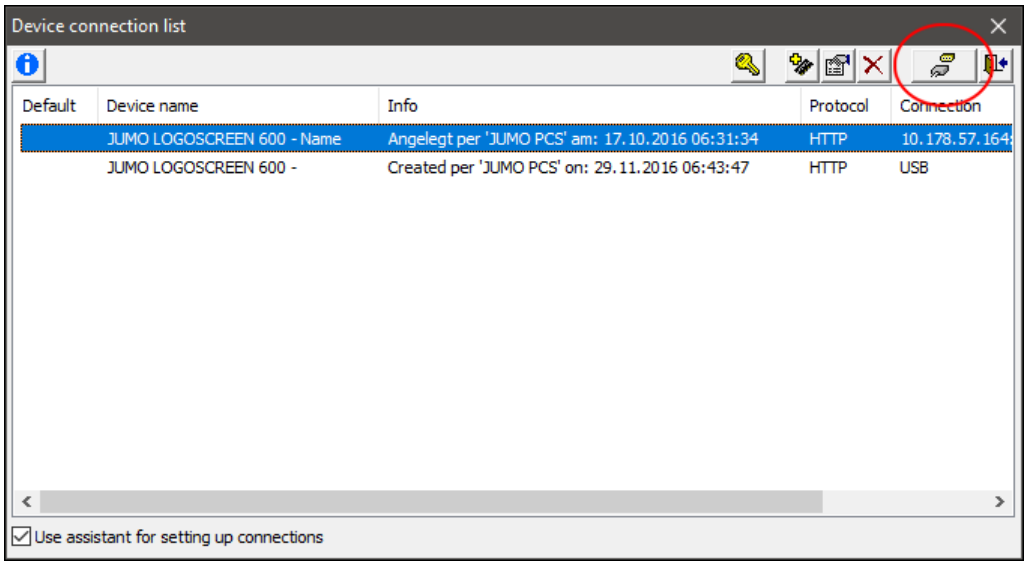
8.1.4 Establish/terminate connection

If a connection has been established and the connection settings defined, the connection between PCS and the device can be established

Establish connection

* Invoke the **DATA TRANSFER > ESTABLISH CONNECTION** command in the menu bar or by clicking the  symbol in the toolbar.

The device connection list is opened.



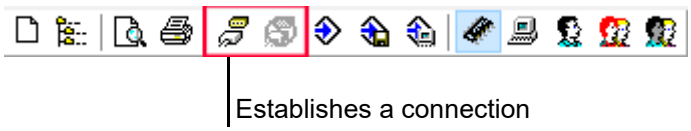
* Select the desired connection in the device connection list and activate via the  symbol.

Connected

PCS and device are now connected. The toolbar changes to...

Terminate connection

* Click the  symbol. The connection is terminated. The toolbar changes to...



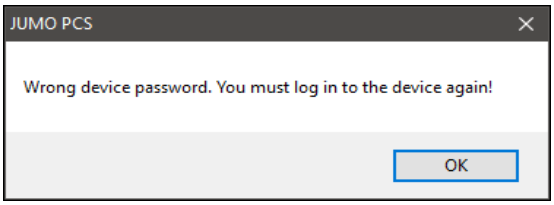
8.1.5 Incorrect logon to the device

If a device is accessed within the setup program, an error may occur when logging on to the device.

For example, the user may not be registered in the device rights file, that the PC and device password may not match or that the device password may have expired (remedy: "Generate/change password", page 28).

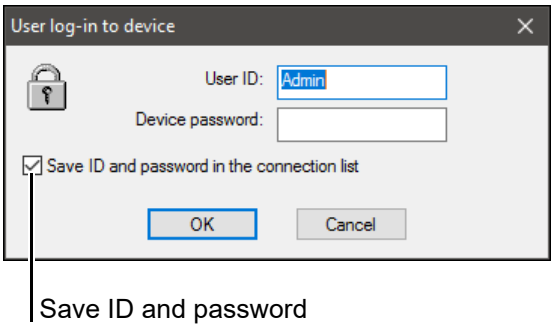
Incorrect logon

The figure below shows an example of a possible error message:



✱ Confirm the error message by pressing the OK button.

A dialog window then appears where the user can log on to the device using a valid device User ID.



Default user

A device with an internal user list including a user is supplied by default.

User: Master Password: 9200

Save ID and password in connection list

If this option is activated (☑), the ID and password are saved and automatically sent to the device the next time a connection is established.

⇨ "Save ID and password", page 99

The ID and password can be deleted from the device list again via the device connection list (features of a connection).

8.1.6 Device rights file for the device

A device rights file can be transmitted to the device via an interface under the following conditions:

- There is a physical connection between the PC of the PCS and the device.

⇨ "Hardware requirements", page 96

- A device connection has been created in the device connection list and the connection settings have been defined.

⇨ "Connection settings wizard", page 97

⇨ "Device connection list", page 101

- The user has the necessary device rights and/or is logged on to the device.

⇨ "Incorrect logon to the device", page 103

The user is in the navigation tree for the view **according to devices**.

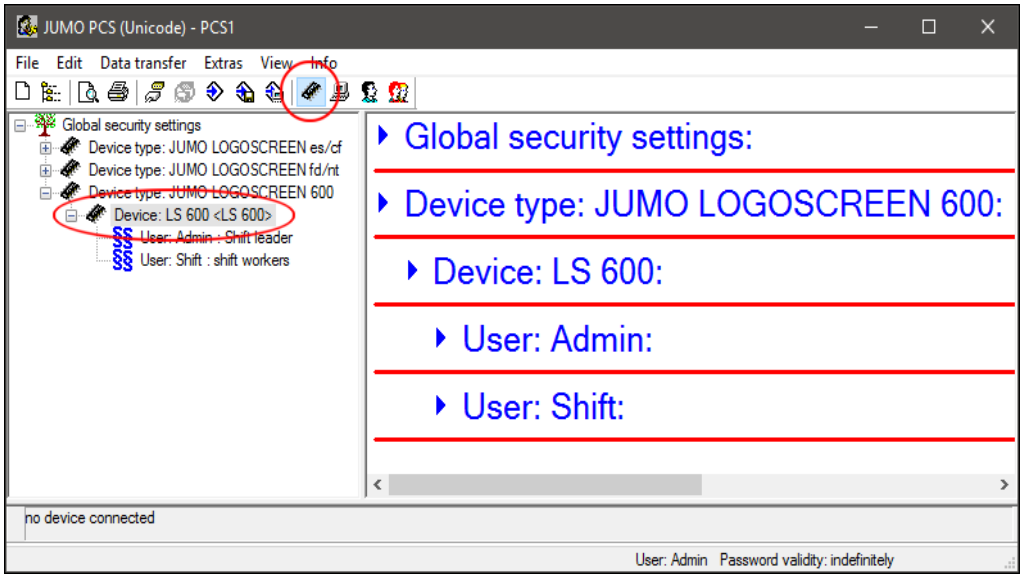
⇨ Chapter 7.2 "View according to devices"

If a connection cannot be established between PCS and the device, the user list can also be transferred to the device as a device rights file using a CompactFlash memory card or a USB flash drive.

⇨ Chapter 8.2 "Transfer via removable disc"

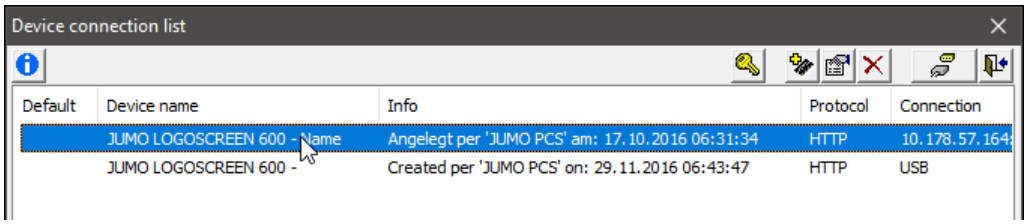
Transfer device rights file

✱ From the navigation tree for the view **according to devices**, select the device to which the user lists need to be transferred as a device rights file.



✱ Invoke the **DATA TRANSFER > DEVICE RIGHTS FILE FOR THE DEVICE** function via the menu bar or by clicking the symbol in the toolbar.

✱ Select the device connection in the device connection list.

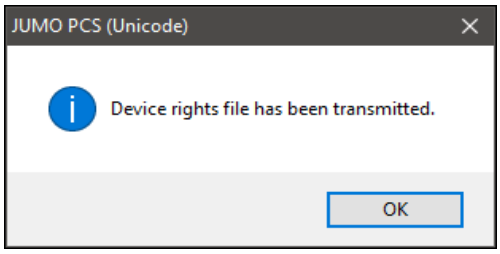


✱ Establish the connection with the device by clicking the  symbol.

The connection to the device is established and the device rights file is transferred to the device.

The connection between PCS on the PC and the device is then terminated again.

If the device rights file has been successfully transferred to the device, the following information appears:



8 Data transfer to the device

8.2 Transfer via removable disc

Security manager software

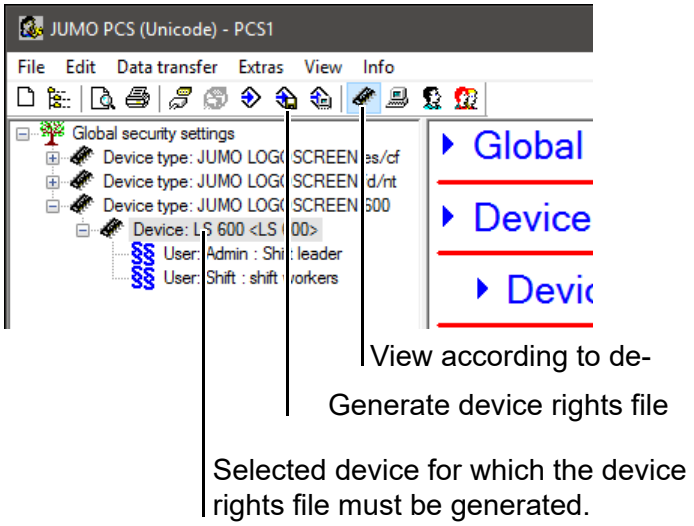
If a connection cannot be established between PCS and the device via an interface, the user list can be transferred to the device as a device rights file using a CompactFlash memory card or a USB flash drive.

8.2.1 Generate device rights file

Requirement for generating a device rights file:

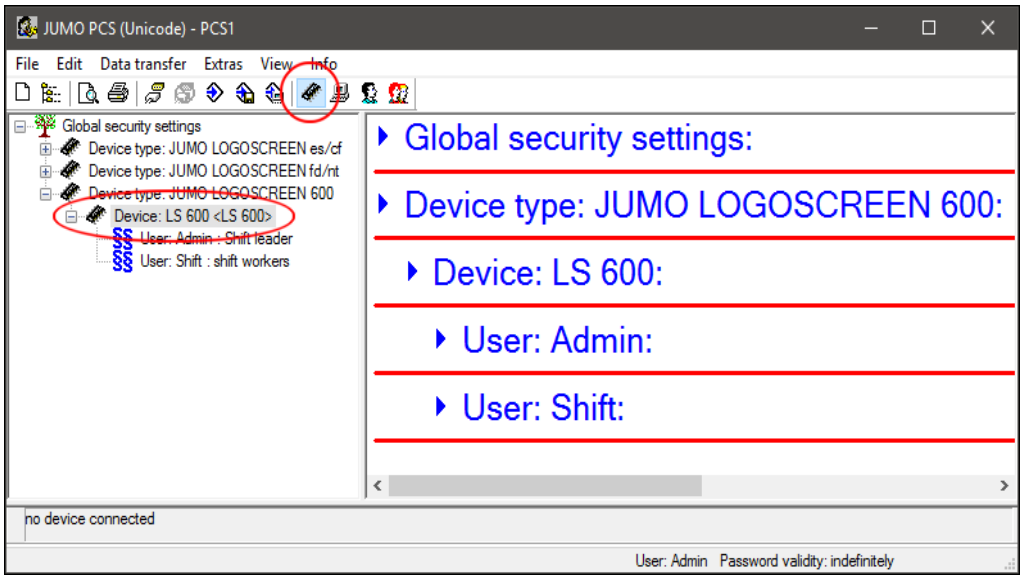
The user is in the navigation tree for the view **according to devices**.

⇨ Chapter 7.2 "View according to devices"

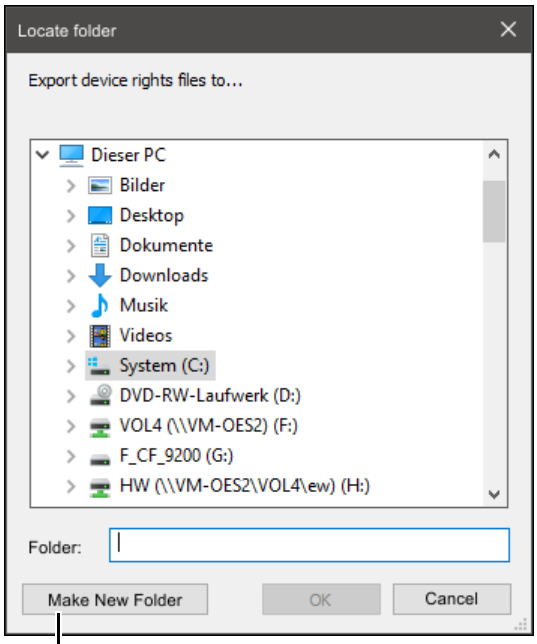


Save device rights file

✱ From the navigation tree for the view **according to devices**, select the device for which the user list needs to be generated and saved as a device rights file.



* Invoke the **DATA TRANSFER > GENERATE DEVICE RIGHTS FILE** function via the menu bar or by clicking the  symbol in the toolbar.



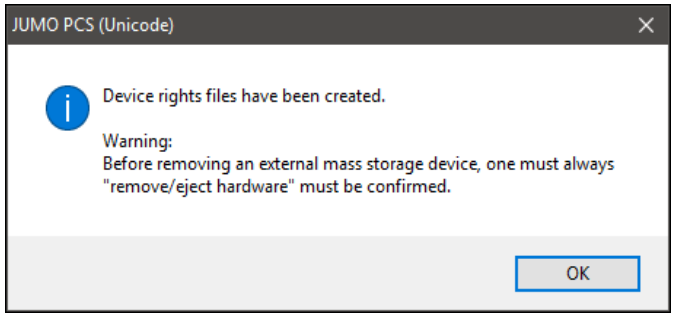
Creates a new folder at the selected storage location

* Select the storage location (target drive) for the device rights file via the **Search folder** dialog window.
* If necessary, create a new folder for the device rights file in the target drive using the Make New Folder button.

If a device rights file needs to be generated and saved directly on a removable disc (CompactFlash card/USB flash drive), this needs to be stored in the removable disc's root directory.

This does not require a selection dialog when loading on the device.

* Confirm folder selection using the OK button.



The device rights file has been generated and stored in the selected folder or on the removable disc.

8 Data transfer to the device

File formats

Depending on the device selection, various file formats are created when generating the device rights file from PCS. This therefore prevents a non-compatible device rights file from being loaded on the respective device via a removable disc.

Device	File format
JUMO LOGOSCREEN es/cf	B17201.set B17202.set
JUMO LOGOSCREEN fd/nt	B18701.set
JUMO LOGOSCREEN 600, 601, 700	KONF323.SET

Only one device rights file for a device can ever be saved on a CompactFlash card or a USB flash drive because the file always has the same name when created and saved from PCS.

This does not require a selection dialog (file selection) on the device.

Loading onto the device

The logged on user must have the "Security - Manage users" right in order to be able to load a new user list onto the device using the USB flash drive or the CompactFlash card.

Important information about loading user lists on the device used can be found in the respective device-specific operating manual.

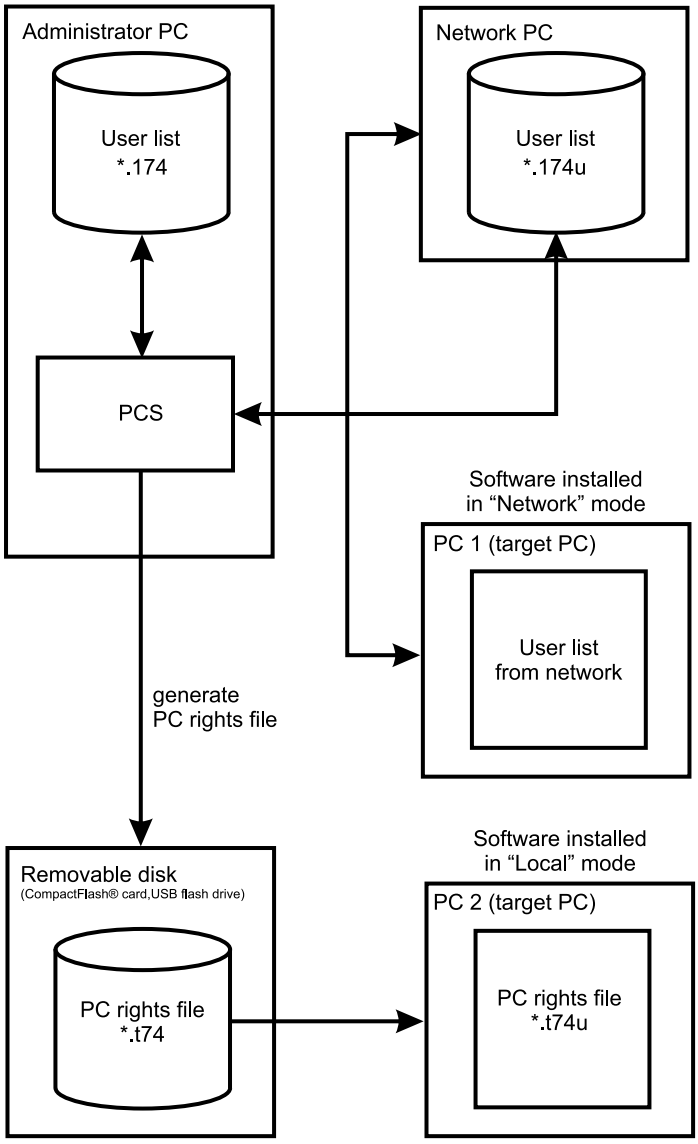
User rights data can be transferred from PCS for PCs with FDA-compliant programs to the target PC as follows:

Direct

- Via Ethernet or serial interface from a network PC where the user list (*.174u) has been stored.

Indirect

- Via a removable disc as a PC rights file (*.t74u) that is stored on a target PC



Install program with the "network user" installation option on the target PC:

⇨ "Installation as "network user"", page 110

Install program with the "local user" installation option on the target PC:

⇨ "Installation as "local user"", page 114

9 Data transfer to a PC

9.1 Transfer via an interface

If programs that use user lists from a central network PC via Ethernet or serial interface need to be installed on a PC or within a network program, the user lists can also be transferred from the administrator PC to the central network PC via an Ethernet or serial interface.

9.1.1 Installation as "network user"

Installation requirements

If a program with the "network user" installation option is installed on the target PC, the following requirements must be met:

- User rights must be generated as a user list (*.174u) in PCS and stored on the network PC that the program accesses.

⇨ Chapter 4.1 "Starting installation"/Chapter 4.2 "Installation options"

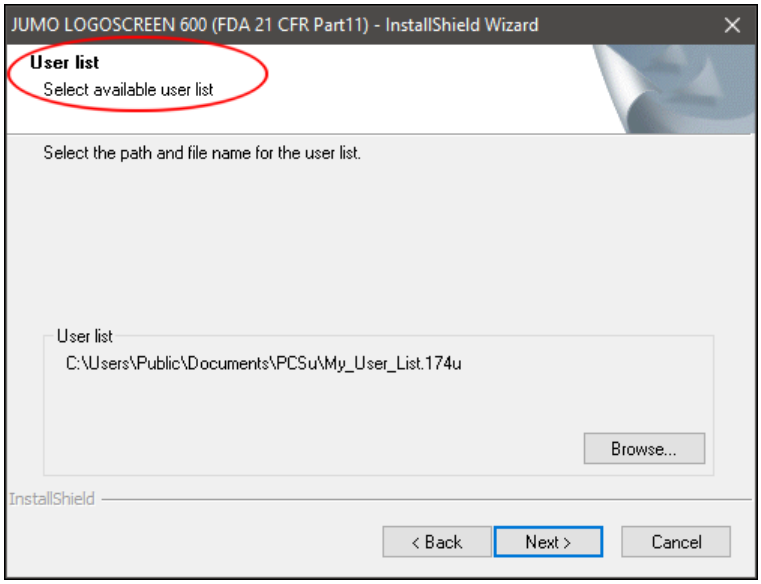
⇨ Chapter 5 "User lists wizard"

⇨ Chapter 7.3 "View according to PCs"

The storage path and file name for the user list are determined during PCS installation ("Administrator", page 17) or when generating a new user list (Chapter 5 "User lists wizard").

Installation

While installing a program on the target PC as a "network user", the path for the user list generated and stored on the network PC is selected and loaded:



The program accesses the user list stored on the network PC during installation and when the program starts up.

Edit user list

If the administrator edits the contents of the user list (and stores it with the same name in the same target directory on the network PC), the edited user list will automatically be available on the target PC after restarting a program.

⇨ Chapter 7 "Edit user lists"

New user list

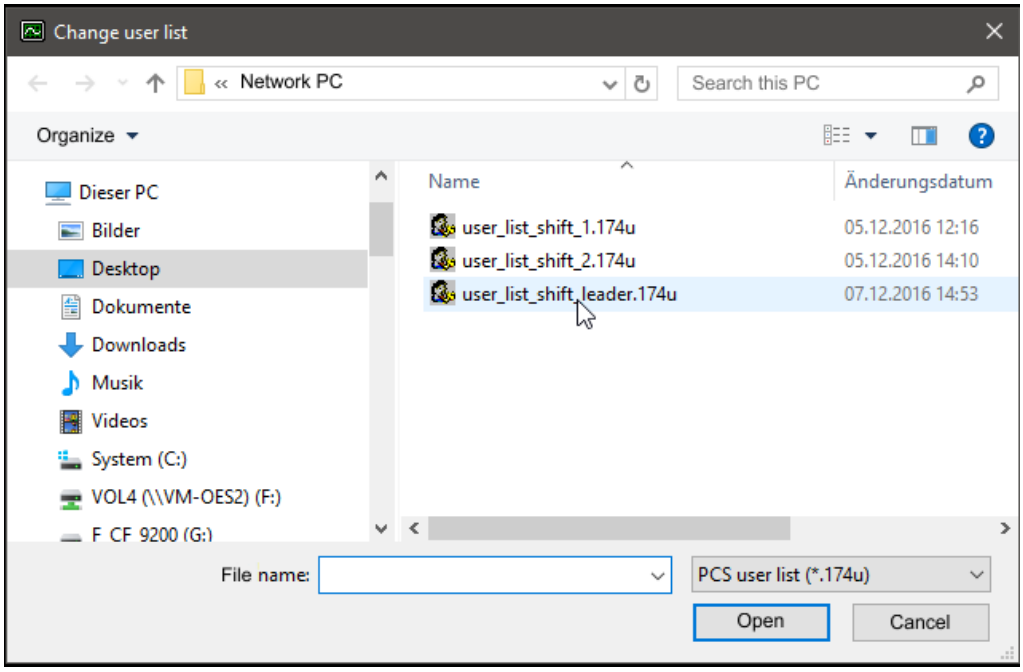
If the administrator creates a new user list on the network PC, this user list can be loaded via the **EXTRAS > RENEW LOGON/CHANGE PASSWORD** menu bar upon reinstallation/restart or in program mode if the user has the necessary rights for this.

Change user list

A user list can be changed via the **EXTRAS > RENEW LOGON/CHANGE PASSWORD** menu bar upon reinstallation/restart or in program mode if the user has the necessary rights for this.

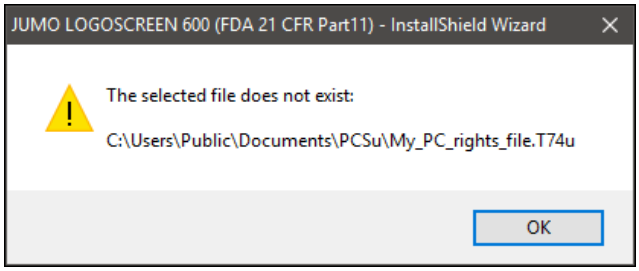
* Activate the "Change user list after logon" option (☑) in the **User log-in** dialog window.

* Select the new user list.



The program starts and accesses the new user list.

9.1.2 Error message upon program start



This error message can be due to the following:

- The user list on the network PC is not (no longer) available.
- The user list has been renamed (after editing/replacement).

Remedy: Store user list (*.174u) with the file name in the target directory that was selected when installing the program ("Installation", page 111).

- There is no network connection between the network PC and target PC or the connection has been interrupted.

Remedy: Establish network connection between the network PC and target PC.

9 Data transfer to a PC

9.2 Transfer via removable disc (local user)

Security manager software

If you cannot establish a connection between PCS and the PC where the program is due to be installed using an interface, you can also transfer the user list to the target PC as a PC rights file using a CompactFlash memory card or a USB flash drive.

9.2.1 Installation as "local user"

Installation requirements

If a program is installed on the target PC using the "local user" installation option, the following requirements must be met:

- User rights need to be generated as a PC rights file (*t74u) in PCS and stored on the PC where the program is installed (target PC) from a removable disc.
- The target PC requires a CompactFlash memory card reader or a USB port.

⇨ Chapter 7.3 "View according to PCs"

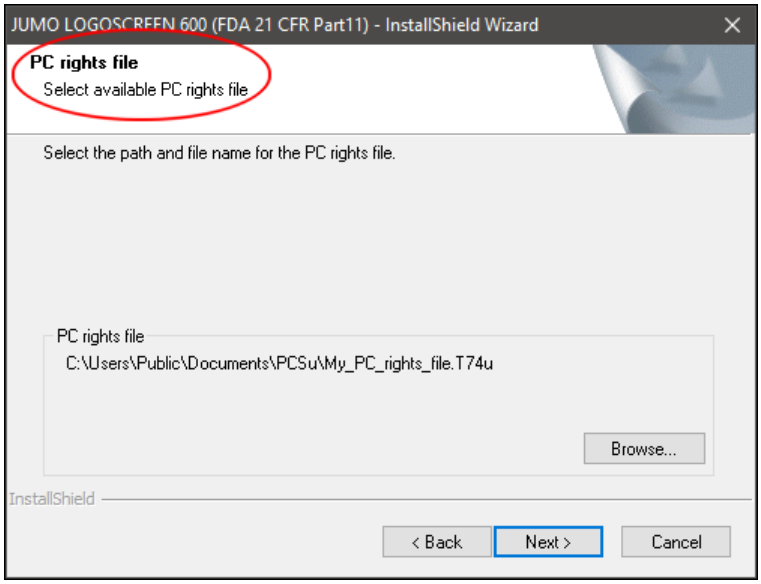
⇨ Chapter 9.2.2 "Generate PC rights file"

The program accesses the PC rights file stored on the target PC during installation and when the program starts up.

If the administrator changes his/her user list, he/she must create new rights files and reload them on the PCs ("local user").

Installation

While installing a program on the target PC as a "local user", the path for the PC rights file generated and stored on the target PC is selected and loaded:



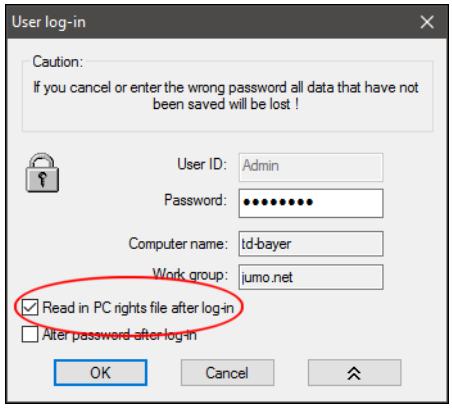
New PC rights file

If the administrator stores a new PC rights file on the target PC, this file can be loaded via the **EXTRAS > RENEW LOGON/CHANGE PASSWORD** menu bar upon re-installation/restart in program mode if the user has the necessary rights for this.

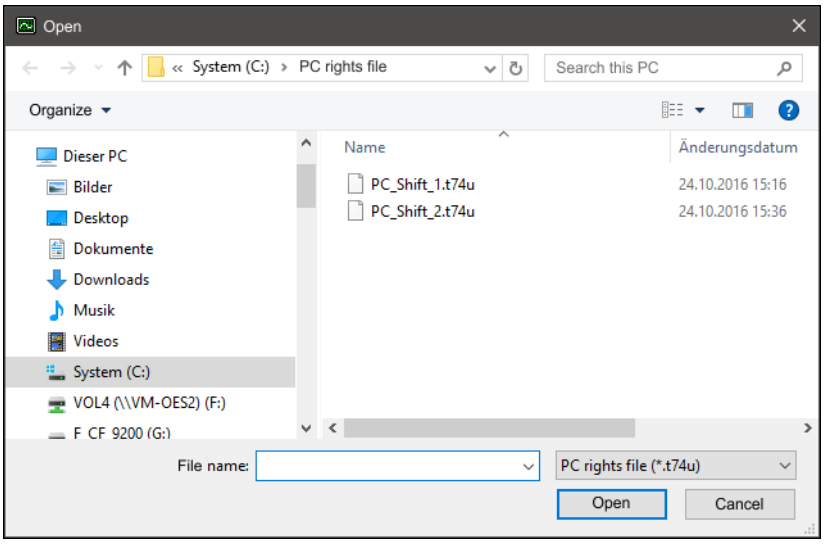
Load PC rights file

A PC rights file can be loaded via the **EXTRAS > RENEW LOGON/CHANGE PASSWORD** menu bar upon reinstallation/restart or in program mode if the user has the necessary rights for this.

✱ Activate the "Load PC rights file after logon" option (☑) in the **User log-in** dialog window.



✱ Select the new PC rights file.



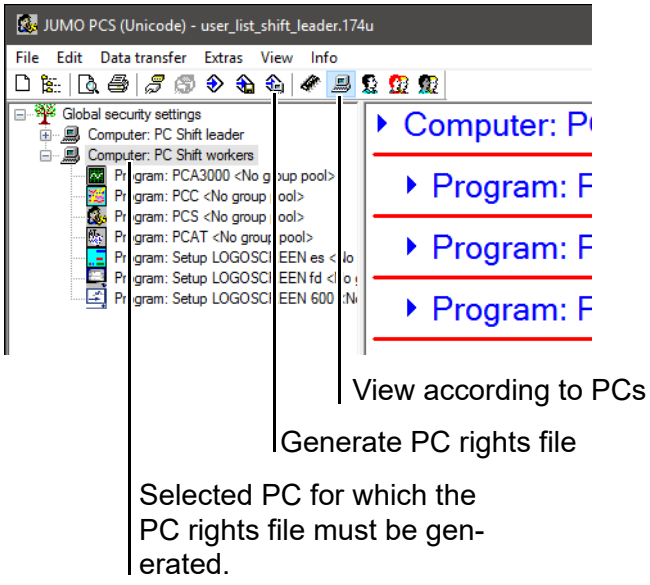
The program starts and loads the new PC rights file.

9.2.2 Generate PC rights file

Requirement for generating a PC rights file:

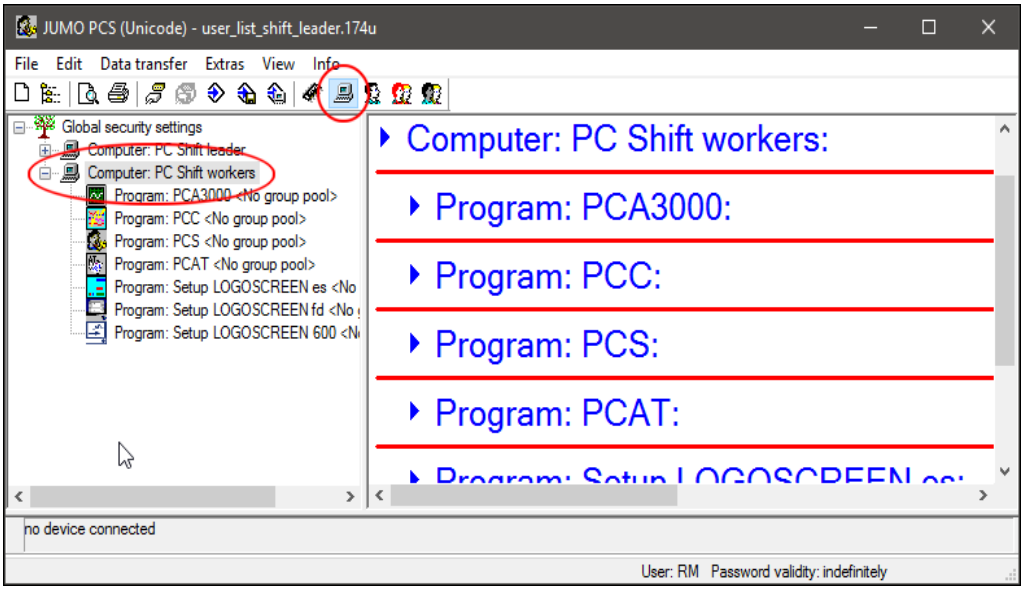
The user is in the navigation tree for the view **according to PCs**.

⇨ Chapter 7.3 "View according to PCs"

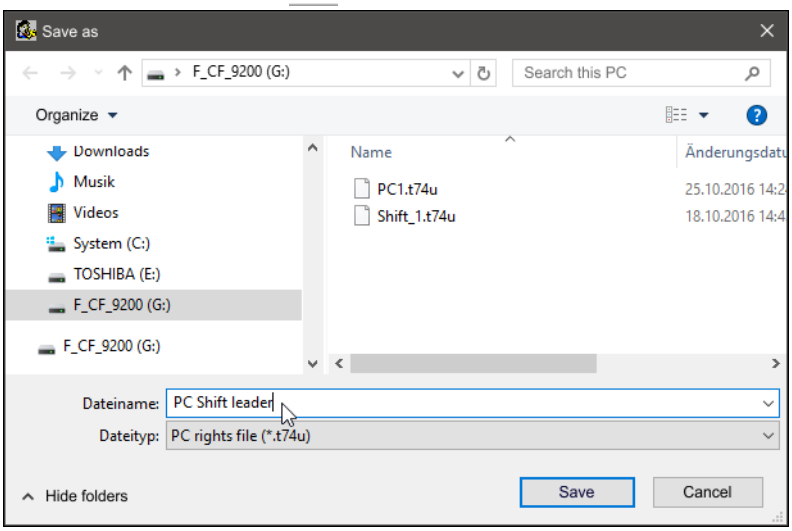


Save PC rights file

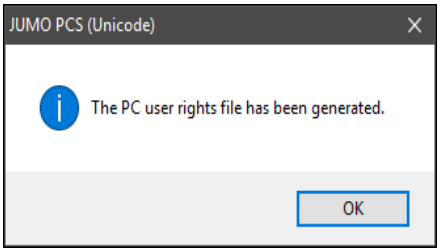
* From the navigation tree for the view **according to PCs**, select the PC for which the user list needs to be generated and saved as a PC rights file.



* Invoke the **DATA TRANSFER > GENERATE PC RIGHTS FILE** function via the menu bar or by clicking the  symbol in the toolbar.



* Select the storage location (target drive) for the device rights file via the **Save as** dialog window, define a file name for the PC rights file and confirm the entry using the Save button.



The PC rights file has been generated and stored in the selected storage location on the administrator PC or on the removable disc.

9 Data transfer to a PC

10.1 File

New user list

The user list wizard is started and a new user list created.

Change user list

Opens and activates an existing user list.

Export as RTF text
The active user list can be saved as an RTF file. The exact contents are determined by the selected line in the navigation tree. The later contents of the RTF file can also be viewed in the dialog window.

The created RTF file can be edited using programs such as Microsoft Word.

Print

Starts the printing process. Depending on the line selected in the navigation tree, there are other filter functions available for the printing process.

Print preview

The "Print preview" function is used to show what a document looks like if printed. Depending on the line selected
in the navigation tree, there are other filter functions available for the print preview of the data.

Printer setup
Opens the **Printer setup** dialog window. Various print options (e.g. paper size) and printer properties (e.g. print quality) can be changed here.

Default settings
Default settings for the program can be changed in the dialog window. The changes only become active after the PC security manager software is restarted.

Exit
Closes the PC security manager software.

10.2 Edit

Edit
Depending on the line selected in the navigation tree and the active view, the entry can be changed using this function. Alternatively: Double-left-click the selected entry in the dialog window.

Remove
Depending on the line selected in the navigation tree and the active view, the entry can be removed using this function. Alternatively: Right-click the selected entry in the navigation tree or dialog window.

New device, New PC, New user, New group pool, New profile

Depending on the active view, a new device, a new PC, a new user, a new group pool or a new profile can be included in the user list. Alternatively: Right-click the selected entry in the navigation tree or dialog window.

New user rights, New profile rights

User rights for accessing a device or a program can be granted in the view according to devices and according to PCs.

Device rights and **program rights** for accessing a device or a program can be granted in the view according to users.

Profile rights for accessing a device or a program can be granted in the view according to profiles.

Alternatively: Right-click the selected entry in the navigation tree or dialog window.

10.3 Data transfer

Establish connection

Establishes a connection to a device. A connection to a device is needed to transfer a rights file from the administrator PC via a interface (serial or Ethernet) to or from the device, network or target PC.

⇨ Chapter 8 "Data transfer to the device"

⇨ Chapter 9 "Data transfer to a PC"

Terminate connection

Terminates an existing network connection. A connection to a device must be terminated before a connection to another device can be established.

Device rights file for the device

A rights file is generated from the current PCS user list for the selected device and sent to the device via an interface (serial or Ethernet). The rights file is evaluated in the device and compared with the user list within the device.
If no connection exists, the software starts access to the default device.

⇨ Chapter 8.1.6 "Device rights file for the device"

User list on the device

Displaying a user list on a device. The device list is not adopted in the current list and cannot be edited. If no connection exists, the software starts access to the default device.

Generate device rights file

Generates a device rights file in the view **according to devices** and stores this file on the hard disc drive or on a removable disc. The device rights file can be loaded on the device via the removable disc. The rights file is evaluated in the device and compared with the user list within the device.

⇨ Chapter 8.2.1 "Generate device rights file"

Generate PC rights file

Generates a PC rights file in the view **according to PCs** and stores this file on the hard disc drive or on a removable disc. This type of rights file must be created if the "local user" installation option is selected when installing a program.

⇨ Chapter 4.2 "Installation options"

⇨ Chapter 9.2.2 "Generate PC rights file"

10.4 Extras

Enable program options

If no valid license number is specified when installing a program, only the demo mode will be active - some of the program's functions will be blocked. This function can be used to subsequently register a program and activate the full version.

Compress user list

Frequently working with a user list (deleting and inserting) means the list (database) on a PC's hard disc drive gets bigger and bigger. This function can be used to build up the user list anew and to save it more compactly (smaller). This has benefits in terms of speed when accessing the list.

Convert user list

This function can be used to convert the user list into the current version.

⇨ Chapter 7.6.7 "Convert user list"

Reset user list on the device

This function should only be used if no users can log on to a device. This is the case if, for example, an incorrect rights file has been sent to a device or if all users have been blocked.

This function is only linked to the rights for the PCS software and not to device rights. If, within the PCS software, the user has the right to execute the function, they will not need to log on to the device.

The function first checks whether a connection to the device exists. If no connection exists, the software tries to establish a connection to a device. If a default device has been defined, this device is used; otherwise a device must be selected from the device list. Logging on to the device is not necessary.

If there is a connection to a device, the device's user list is reset to the default setting. The default setting contains the Master user (password: 9200).

Delete internal memory in the device

Deletes a device's internal memory and reinitializes it. This can be useful, for example, after a test phase - the test data is deleted.

Renew logon/change password

This function allows the logged on user to renew log-in and use the options that are also available when the software is restarted.

⇨ Chapter 5.4 "Options for program start"

CANCEL immediately closes the software.

This function can also be used if the rights/global security settings for the logged in user have been changed. The changed rights are only reinitialized and identified after logging on again.

Comment in audit trail

This function can be used to create a manual audit trail entry. The entries can be visualized with the PC Audit Trail Manager software.

⇨ Further information about the PC Audit Trail Manager software (PCAT) can be found in the B 70.9704.0 operating manual.

Device audit trails are evaluated by the PC Evaluation Software (PCA3000).

10.5 View

According to devices

View of all available devices.

⇨ Chapter 7.2 "View according to devices"

According to PCs

View of all available computers.

⇨ Chapter 7.3 "View according to PCs"

According to users

View of all available users.

⇨ Chapter 7.4 "View according to users"

According to group pools

View of all available group pools.

⇨ Chapter 7.5 "View according to group pools"

Update

The screen contents are reloaded.

Connection status

Displays the status of the device connection.

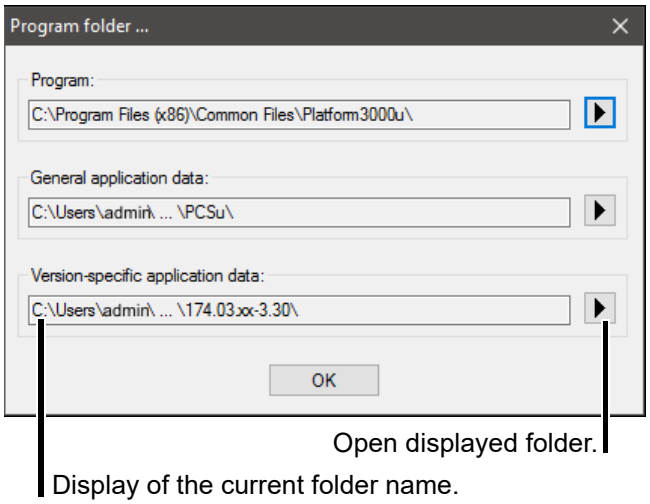
⇨ "Connection status", page 36

10.6 Info

Info about ... This window shows information about the version number of the program. This number is important if you contact telephone support with technical questions.

Registered license numbers ... This window shows information on the license number of the program. This number is important if you contact telephone support with technical questions.

Program folder ... This window displays information about the currently selected folder that the program accesses by default (default directory for user lists).



Open displayed folder.

Display of the current folder name.

10 Menu functions & symbols

A

C

D

E

G

H

I

K

L

M

N

P

R

S

T

U

V

W

JUMO GmbH & Co. KG
Street address:
Moritz-Juchheim-Straße 1
36039 Fulda, Germany
Delivery address:
Mackenrodtstraße 14
36039 Fulda, Germany
Postal address:
36035 Fulda, Germany
Phone: +49 661 6003-0
Fax: +49 661 6003-607
Email: mail@jumo.net
Internet: www.jumo.net

JUMO Instrument Co. Ltd.
JUMO House
Temple Bank, Riverway
Harlow, Essex, CM20 2DY, UK
Phone: +44 1279 63 55 33
Fax: +44 1279 62 50 29
Email: sales@jumo.co.uk
Internet: www.jumo.co.uk

JUMO Process Control, Inc.
6733 Myers Road
East Syracuse, NY 13057, USA

Phone: +1 315 437 5866
Fax: +1 315 437 5860
Email: info.us@jumo.net
Internet: www.jumousa.com