Miltenyi Biotec

CliniMACS® Plus Software

User manual



The CliniMACS System components, including Reagents, Tubing Sets, Instruments, and PBS/EDTA Buffer, are designed, manufactured and tested under a quality system certified to ISO 13485. In the EU, the CliniMACS System components are available as CE-marked medical devices for their respective intended use, unless otherwise stated. In the US, the CliniMACS CD34 Reagent System, including the CliniMACS Plus Instrument, CliniMACS CD34 Reagent, CliniMACS Tubing Set TS and CliniMACS Tubing Set LS, and the CliniMACS PBS/EDTA Buffer, is FDA approved as a Humanitarian Use Device (HUD), authorized by U.S. Federal law for use in the treatment of patients with acute myeloid leukemia (AML) in first complete remission. The effectiveness of the device for this indication has not been demonstrated. Other products of the CliniMACS Product Line are available for use only under an approved Investigational New Drug (IND) application, Investigational Device Exemption (IDE) or FDA approval. In Australia, the following components of the CliniMACS Plus System are included in the Australian Register of Therapeutic Goods (ARTG) and are therefore approved for supply: CliniMACS Plus Instrument, CliniMACS CD34 Reagent, CliniMACS Tubing Set, CliniMACS Tubing Set LS, CliniMACS Depletion Tubing Set and CliniMACS PBS/EDTA Buffer. Only those products which are included in the ARTG may be used in Australia.

Unless otherwise specifically indicated, Miltenyi Biotec products and services are for research use only and not for therapeutic or diagnostic use.

Copyright © 2026 Miltenyi Biotec and/or its affiliates. All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, transmitted, published, or distributed in any form or by any means, electronically, mechanically, by photocopying, microfilming, recording, or otherwise, without the prior written consent of Miltenyi Biotec; however, notwithstanding the foregoing, the owners of the instrument may make copies solely for purposes of training personnel in the use and servicing of the unit within their business or organization.

CliniMACS Plus Software

User manual

Software version 3.0

Issued: 2026-09
210-005-795/01

MD CE 0123

Miltenyi Biotec B.V. & Co. KG
Friedrich-Ebert-Straße 68
51429 Bergisch Gladbach
Germany

Miltenyi Biotec Technical Support
+49 2204 8306-3803
technicalsupport@miltenyi.com
www.miltenyibiotec.com

Table of contents

1 About this user manual 7

1.1 Read the manual first 7

1.2 Associated documents 7

1.3 Presentational conventions 8

1.3.1 Text styles 8

1.3.2 Screens and figures 8

2 Safety information 9

2.1 Instrument related safety notes 9

2.2 Software related safety notes 9

2.3 Hazards 10

2.3.1 Hazard levels 10

2.3.2 Structure of warning messages 10

3 Cybersecurity 13

3.1 Defense-in-depth concept for security 13

3.1.1 Physical protection layer 14

3.1.2 Network environment layer 15

3.1.3 Instrument software layer 16

3.1.4 User layer 17

3.1.5 Auditing layer 17

3.1.6 Update handling layer 18

3.1.7 Vulnerability handling layer 18

3.1.8 Backup- and recovery layer 18

3.2 Summary of secure configuration 18

4 Software concept 19

4.1 Regulatory information 19

4.2 Data protection laws 19

4.3 Basic concept 19

4.3.1 Application process 20

4.3.2 Tool 20

4.3.3 Setting 20

4.4 Graphical user interface 21

4.4.1 Menu bar and content area 21

4.4.2 Status line 22

4.4.3 Toolbar 22

4.4.4 Input fields 23

4.4.5 Pop-up windows 23

5 Basic operation 25

5.1 Switching on the instrument 25

5.2 Login 26

5.3 Logout 26

5.4 Shutting down the instrument 26

5.5 Emergency stop 27

5.6 Selecting an application process 27

5.7 Executing an application process 28

5.8 Pausing an application process 29

5.9 Viewing the status of the instrument and of the application process 30

6 Data access 31

6.1 Retrieving application logs 31

6.1.1 Viewing and exporting log files to USB flash drive 31

6.1.2 Retrieving files via file sharing 33

6.2 Retrieving audit trail 33

6.2.1 Viewing audit trail 34

6.2.2 Exporting audit trail 34

6.2.3 Deleting audit trail 36

7 Tools and user settings 37

7.1 Accessing tools and user settings 37

7.2 Tools 37

7.2.1 Backup filed data 38

7.2.2 Custom files 39

7.2.3 Info 39

7.2.4 Instrument check 39
7.2.5 License 39
7.2.6 Sealer 39
7.2.7 Shutdown 39
7.2.8 UMS file exchange 40
7.3 User settings 40
7.3.1 Customer settings 41
7.3.2 Network settings 41
7.3.3 Network utilities 41
7.3.4 Set time 41
7.3.5 Settings exchange 41
7.3.6 SetVolume 42
7.3.7 UMS settings 42

8 Network integration 43
8.1 Connecting to a local network 43
8.2 Connecting to an LDAP server 45
8.3 Connecting to a network drive 46
8.4 Connecting to an email server 48
8.5 Enabling network time synchronization 50

9 User management 53
9.1 General information 53
9.1.1 Rights 53
9.1.2 Roles 53
9.1.3 Accounts 54
9.2 Managing roles and accounts 55
9.2.1 Accessing the user management system 55
9.2.2 Creating a new role 56
9.2.3 Changing rights of roles 57
9.2.4 Adding local users 57
9.2.5 Adding LDAP users 59
9.2.6 Adding LDAP groups 60
9.2.7 Changing assigned roles of users or LDAP groups 61

9.2.8 Deactivating local users 61
9.2.9 Deleting LDAP users 61
9.3 Configuring password policy 61
9.4 Importing and exporting user management settings 62
9.4.1 Exporting user management settings 63
9.4.2 Importing user management settings 65

10 Troubleshooting 67
10.1 Service information 67
10.2 Miltenyi Biotec Technical Support 67
10.3 Error messages 67
10.3.1 Login issues 68

11 Legal notes 69
11.1 Limited warranty 69
11.2 Trademarks 70

12 Appendix 71
12.1 Glossary 71
12.1.1 Abbreviations 71
12.1.2 Terms 71
12.2 Roles and rights 72

1

About this user manual

This chapter provides general information about the importance of reading this user manual before using the instrument. It also covers the associated document series and the presentational conventions used in this manual.

This user manual provides instructions, warnings, precautions, and other important information for the setup and safe operation of the CliniMACS Plus core software. Make sure to use the software manual that corresponds to the software version installed on the instrument.

For further details on the instrument hardware, refer to the CliniMACS Plus Instrument user manual, for further details on the processes running on the instrument, refer to the CliniMACS Plus Applications user manual.

1.1 Read the manual first

⚠ WARNING

Risk of electrical shock, physical injuries, instrument damage, or malfunction.

Disregard of any instructions, warnings, or cautions at any time can endanger users and others and may compromise the electrical, electronical, electromagnetic, and mechanical safety. Disregard also excludes the manufacturer from any liability.

- The operation of the instrument must be performed by trained users only.
- Before using the instrument carefully read and understand the safety information, warnings, precautions, and instructions for proper operation provided in the CliniMACS Plus Instrument user manual and in any safety-related recommendations issued by Miltenyi Biotec.
- Pay special attention to all warnings shown on the instrument or provided with consumables and accessories.
- Adhere to all safety information, warnings, precautions, and instructions at all times while the instrument is in operation.
- Retain the user manuals for future reference. They should be kept accessible and readily available together with all other safety and operating documentation during the entire life cycle of the instrument.

1.2 Associated documents

This user manual is part of a series and should only be used in conjunction with the other user manuals of the series.

- CliniMACS Plus Instrument user manual
- CliniMACS Plus Applications user manual

- MACS® TubeSealer user manual

1.3 Presentational conventions

The following text styles are used to indicate specific information types in this user manual that are not safety-related. For safety-related information types, see section 'Hazard levels' and section 'Structure of warning messages'.

1.3.1 Text styles

• Bullet point list item with text	Indicates a list-item of an unordered list
1. Numbered list item with text	Indicates a list-item of a step-by-step instruction
Bold, colored text	Indicates a software element (for example a button or tab of the graphical user interface)
See section 'Text styles'	Indicates a reference to the section with the heading 'Text styles'
See Figure 4.2/Table 4.2	Indicates a reference to the second figure/table in chapter four

IMPORTANT:
Advises the user of important practices or information not related to personal injury nor property damage

1.3.2 Screens and figures

The screens and the figures in this manual are only representative screens and may slightly differ from those shown on the instrument.

2

Safety information

This chapter states safety notes to ensure the safe use of the CliniMACS Plus Software.

2.1 Instrument related safety notes

For detailed information on the safe use of the instrument, refer to the CliniMACS Plus Instrument user manual.

2.2 Software related safety notes

IMPORTANT:
The access control of the instrument must be validated before use. Keep username and password safe. It is recommended to establish a so-called 'break-glass-solution' (see chapter 'User management'). In case of failed login during a process run, contact Miltenyi Biotec Technical Support.

- Before using the instrument, read the 'Safety information' chapter in the CliniMACS Plus Instrument user manual and the information contained in this software user manual, including any safety notes and operating instructions.
- Pay special attention to all warnings shown on the instrument.
- Failure to read and observe these guidelines can lead to improper or incorrect usage and result in damage to the instrument. Improper usage could also cause severe personal injury, death, unpredictable results, instrument malfunction, and premature wear of components shortening the lifetime of the instrument. Such actions may void the warranty.
- Keep the user manual and any other safety and operating instructions provided with the instrument in a safe place accessible to all users for future reference.
- All processing procedures must be performed by trained users only. The user must have a general understanding of cell processing and knowledge about biosafety.
- Only authorized local Miltenyi Biotec service providers should install, maintain, or service the instrument.
- The communication and data access between the software and an external server/application must be validated before use.
- In case of a serious concern regarding the safe use of the instrument, contact Miltenyi Biotec Technical Support.
- In case of problems or failures, contact Miltenyi Biotec Technical Support.

2.3 Hazards

2.3.1 Hazard levels

The color and signal word of a warning message depend on the hazard level. The hazard level classifies the hazard as follows:

⚠ WARNING

indicates a hazardous situation that, if not avoided, could result in death or serious injury.

⚠ CAUTION

indicates a hazardous situation that, if not avoided, could result in minor or moderate injury.

NOTICE

indicates a hazardous situation that, if not avoided, could result in property damage. This does not indicate a risk of personal injury.

2.3.2 Structure of warning messages

Warning messages warn of hazardous situations. Warning messages specify the hazard level, the type and source of the hazard, the possible consequences, and the measures to avoid the hazard.

The following examples show the structure of warning messages at the beginning of a chapter or section where a hazard can occur:

⚠ WARNING

Type and source of hazard.

Consequences of noncompliance.

- Measures to avoid the hazard.

⚠ CAUTION

Type and source of hazard.

Consequences of noncompliance.

- Measures to avoid the hazard.

NOTICE

Type and source of hazard.

Consequences of noncompliance.

- Measures to avoid the hazard.

The following examples show the structure of embedded warning messages before an instructional step:

1. **WARNING! Type and source of hazard. Consequences of noncompliance. Measures to avoid the hazard.** Instructional step.

1. **CAUTION! Type and source of hazard. Consequences of noncompliance. Measures to avoid the hazard.** Instructional step.

1. **NOTICE Type and source of hazard. Consequences of noncompliance. Measures to avoid the hazard.** Instructional step.

3

Cybersecurity

This chapter describes the measures for cybersecurity and the eight layers of the core software's defense-in-depth concept.

3.1 Defense-in-depth concept for security

Cybersecurity is a shared responsibility between Miltenyi Biotec and the users. The software is designed with built-in security measures to protect against common threats. Users must play an active role in safeguarding the data and maintaining secure practices. In alignment with the intended purpose, a defense-in-depth concept is recommended. The goal of this concept is:

- Preventing negative impact on cell product quality and delay of cell product
- The integrity of protocols, processes, and audit data
- The integrity of the instrument configuration
- Availability of the instrument for cell processing
- Allowing access only by trained and authorized users

The defense-in-depth model is structured in the following layers (see Figure 3.1):

- Physical protection layer
- Network environment layer
- Instrument software layer
- User layer
- Auditing layer
- Update handling layer
- Vulnerability handling layer
- Backup- and recovery layer

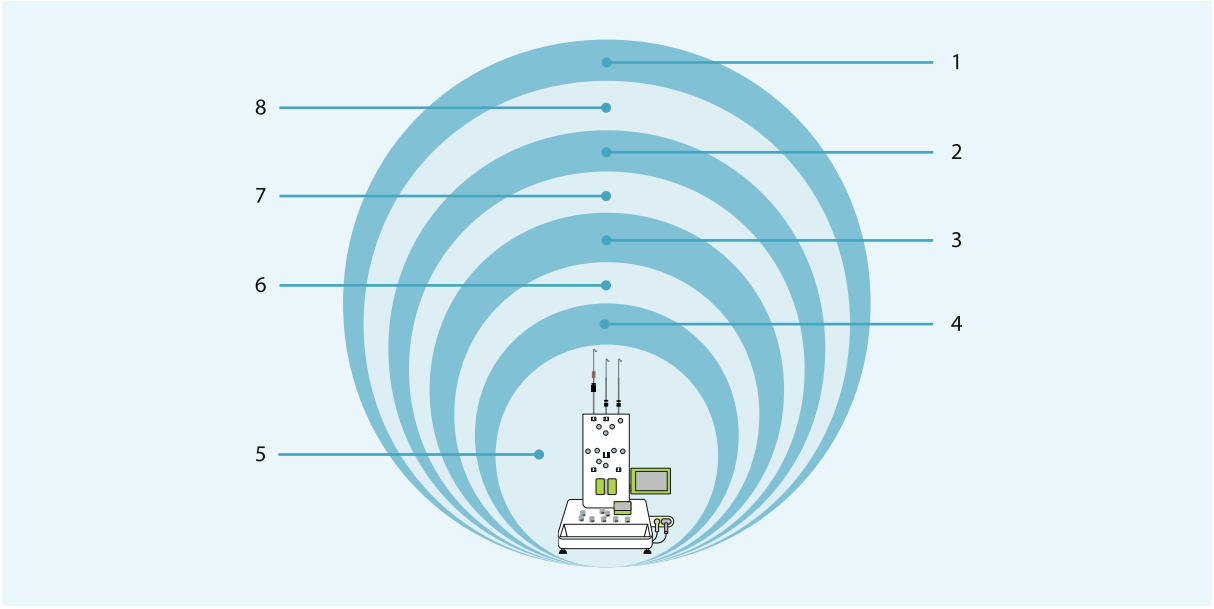


Figure 3.1: Layers of the defense-in-depth concept

1 Backup- and recovery layer
2 Update handling layer
3 User layer
4 Network environment layer
5 Physical protection layer
6 Instrument software layer
7 Auditing layer
8 Vulnerability handling layer

3.1.1 Physical protection layer

The instrument is equipped with the following physical interfaces which support the connection of different components, accessories, and external devices (see Table 3.1). The customer is responsible to ensure that only authorized personnel have physical access to the product and to provide suitable processes to control and monitor physical access.

Interface	Purpose
Alarm connector	Interface for the connection to an external alarm system. No data interface
CAN port	Interface for the connection to additional devices
Ethernet port	Interface for the connection to a network
Touchscreen	Data input device used by users and service personnel to operate the instrument
Tube sealer connector	Interface for the connection to the MACS®TubeSealer, a heat sealer installed on the instrument. No data interface
USB port	Interface for the connection to approved peripherals (for example the external keyboard or the barcode reader) and USB flash drives. Latter can be used for transferring protocols and log files from the instrument and for bringing programs and updates to the instrument

Table 3.1: Interfaces and peripherals of the instrument

IMPORTANT:
Only USB flash drives formatted as FAT32 are supported.

The USB ports allow the connection of USB flash drives. Even though operating system and application measures are in place to manage USB connections, it is the responsibility of the customer to ensure that only approved and controlled USB flash drives are used with the instrument.

Improper handling (for example physical force) of interfaces or accessories can damage the physical interfaces of the instrument and render them non-functional and constitute a remaining risk.

3.1.2 Network environment layer

The instrument shall be used in a protected network segment that is separated from other segments. A possible setup in which the instrument is part of an isolated instrument network is depicted in Figure 3.2. A router separates the different network segments from each other and controls the data flow between them.

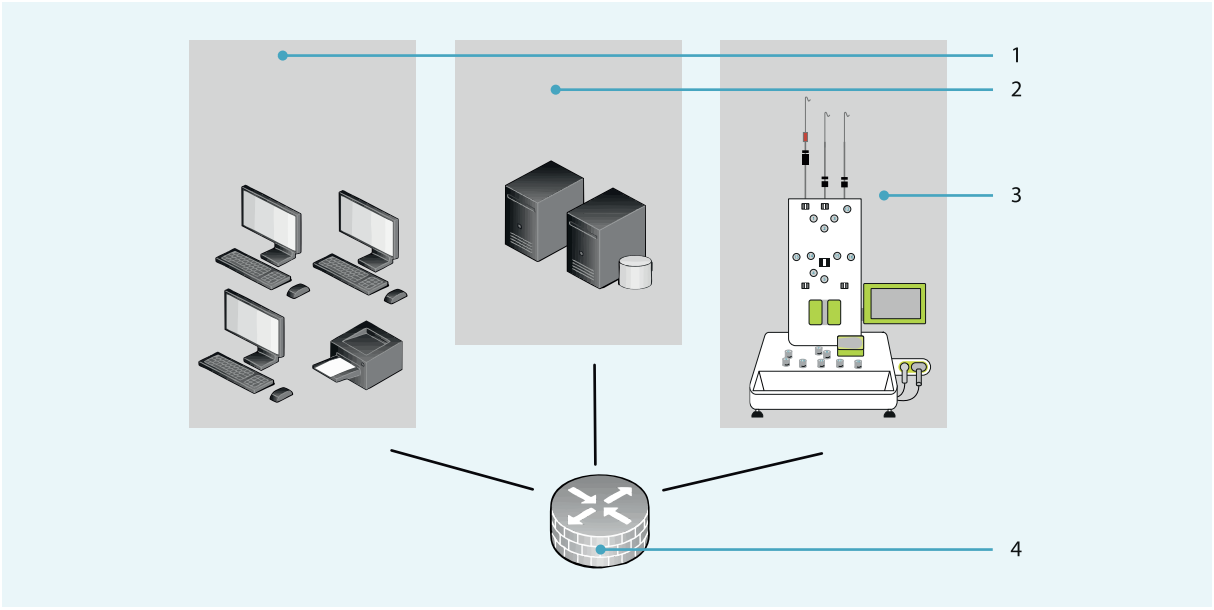


Figure 3.2: Network diagram (exemplary)

1 General corporate network
2 Protected central service (network services, for example DHCP, DNS, LDAP, and NTP)
3 Protected instrument network (CliniMACS Plus)
4 Router

The instrument mainly provides functions to connect to other systems on the network. The supported network protocols are listed in Table 3.2.

Interface	Purpose	Port	Comment
NTP	Time synchronization	123	–
DNS (client)	Resolve host names to IP addresses	53 (UDP)	–
ICMP echo request/ response (server)	Check network connectivity to the instrument	N/A	–
DHCP (client)	The automatic network configuration of the instrument	68 (UDP)	–
LDAP	Login to the instrument with centrally managed active directory credentials	389	Insecure protocol, only use if LDAPS is not supported
LDAPS	Secured version of LDAP	636	A secure variant of LDAP. Requires proper configuration, see section 'Connecting to an LDAP server'.
SMB	File Sharing	445	Authenticated share is supported. Requires configuration, see section 'Connecting to a network drive'.
SMTP	Email notification	25, 2525, 465, 587	Authentication is supported, Requires proper configuration, see section 'Connecting to an email server'.
SMTPS	Secured version of SMTP	465, 587	A secure variant of SMTP. Requires proper configuration, see section 'Connecting to an email server'.

Table 3.2: Network connections and protocols

IMPORTANT:
Secure protocols are supported for all services. It is strongly advised to only activate the secure functions listed in Table 3.2. For compatibility reasons, insecure versions of protocols are supported. In cases where the insecure protocol is needed for compatibility reasons, proper mitigating measures must be applied by the customer.

The customer is responsible to ensure only authorized personnel have network access to the instrument and the networks used to transfer the activated protocols. Suitable processes to control and monitor network access must be in place. In addition, the instrument must not be directly exposed to the Internet.

3.1.3 Instrument software layer

A customized Linux operating system is used on the instrument. Only required software, services, and kernel features are enabled to minimize the attack surface of the instrument software.

Access to the BIOS of the instrument's PCs is only available to Miltenyi Biotec trained service personnel. The configuration of the BIOS prevents booting from external media to ensure the integrity of the instrument software.

Measures are in place to ensure that only authorized software can be run on the instrument. New software is installed on the instrument using a USB flash drive. The automatic start of software from the USB flash drive is prevented and a user cannot start applications directly from a USB flash drive.

Additional software that shall be generally available on the instrument, needs to be installed using an installer delivered with this software. To ensure that only the original software of Miltenyi Biotec intended for the instrument can be installed, several checks are in place. More specifically, the installer checks the expiration date of the installation package and the electronic signature of the software to be installed on the instrument. If a check fails, the software cannot be installed. Before running the installation, the software package needs to be copied into volatile memory on the instrument using the Custom Files tool. This tool

ensures that besides the proprietary executable formats only original files signed by Miltenyi Biotec can be copied to the instrument for execution.

The installation of a new instrument software version is described in section 'Update handling layer'. Core software updates are performed by Miltenyi Biotec's service personnel, new applications by field application specialists.

There is no distinct malware detection software running on the system, as this is not suitable for this product. Instead, the risk of malware is controlled via this defense-in-depth concept.

Application software and tools validate user inputs for plausibility. Such validation contains, among others, range validation for numeric inputs, validation of consumable lot and product numbers, and plausibility checks for entries.

The software and applications are not requested during operation to provide personal health information. A low risk remains that it is entered during the application run by the user. It is the responsibility of the user to ensure that applicable privacy-related regulations are followed.

Protocols and log data can be exported from the instrument. The exported data is accompanied by file hashes to allow the user to check that the export and transfer to a downstream system were successful and that no transfer-related data corruption occurred. Currently, the used algorithm is MD5.

Access to software intended for maintenance purposes and to restricted functionality of application processes is available to Miltenyi Biotec personnel only. Users do not have access during normal operations. Access is possible with the service account, a service USB flash drive, or through the remote access functionality of the Info tool in combination with a one-time PIN. Only Miltenyi Biotec has access to the credentials of the service account and the service USB flash drive. The service USB flash drive is a flash drive with authentication information and an associated PIN. For troubleshooting purposes, a Miltenyi Biotec service engineer can access the instrument with a USB flash drive and a one-time PIN provided by Miltenyi Biotec Technical Support.

IMPORTANT:
There is no protection in place to protect the exported data from being read or intentionally manipulated. The customer must ensure that only authorized personnel has access to the exported data.

3.1.4 User layer

The access to the instrument can be protected via configurable user management (see chapter 'User management'). The customer must ensure that the instructions and recommendations outlined in this document are implemented.

In addition, the customer must ensure that only trained and authorized personnel are given access to the instrument and that common best practices regarding usage of passwords and applicable regulations are being followed.

3.1.5 Auditing layer

The audit trail system (ATS) logs information about actions performed on the instrument, for example user entries during an application run or changes to the configuration of the instrument. When the audit trail is enabled, actions are logged in the audit trail of the instrument. The customer must ensure that the instructions and recommendations outlined in this document are followed.

Even though audit trail data is generated by the instrument, improper handling of audit trail data is a remaining risk. To mitigate the risk, the customer is responsible for the security and handling of audit trail data (for example export, storage, deletion, and review) following applicable regulations.

3.1.6 Update handling layer

Security updates are shipped in the context of update packages. Miltenyi Biotec will inform the customer when a new software is available.

Instrument software updates must be performed by Miltenyi Biotec's service personnel only. The instrument software updates are delivered and installed following procedures outlined in Miltenyi Biotec's SOPs. Updates are packed in dedicated packages containing the new instrument software and the software performing the actual installation. Updates are delivered via a USB flash drive. To ensure the integrity of the package all components are cryptographically signed and checked before installation. Contact Miltenyi Biotec Technical Support for scheduling an update of the instrument.

3.1.7 Vulnerability handling layer

To report a security vulnerability or an incident affecting the product or one of its components, contact the Miltenyi Biotec Technical Support (see chapter 'Troubleshooting').

3.1.8 Backup- and recovery layer

The instrument only provides the functionality to backup protocols and data. The customer must make sure that a data backup is made regularly and follows applicable regulations. In case the instrument software becomes inoperable, contact Miltenyi Biotec Technical Support.

3.2 Summary of secure configuration

The previous sections introduce security measures that are in place and recommend measures to set up for the secure operation of the CliniMACS Plus. These measures fall into two categories: configuration of instrument and procedures and policies that enhance the security of the instrument. The following measures are recommended:

- Ensure that only authorized personnel have access to the instrument and its interfaces.
- Ensure that access to the network, in which the instrument is operated, is limited to authorized personnel and systems.
- Enable authentication and authorization on each instrument to ensure that only authorized personnel can access the instrument software.
- The customer must have an appropriate authorization management in place to ensure that personnel using or accessing the instrument are assigned only the rights needed to perform the job function (least privilege principle).
- Set up a suitable password policy to follow best practices and comply with applicable regulations.
- Secure protocols should be preferred over insecure variants.
- Processes and procedures must be set up to ensure that only approved and controlled USB flash drives are used and that the use of other USB flash drives is prevented.
- Processes and procedures must be in place to ensure the adequate handling of audit trails, protocols, and log data following applicable regulations.
- Personnel must be trained in security awareness and basic security hygiene.
- Processes and procedures must ensure that backups of the instrument's data are made regularly and follow applicable regulations.
- It is the customer's responsibility that no personal health information is used on the instrument.

4

Software concept

This chapter states regulatory information and information regarding data protection laws. It also describes the basic concept of the instrument software and the graphical user interface (GUI).

4.1 Regulatory information

The software is developed according to standard IEC/EN 62304. In addition, the CliniMACS Plus core software has been developed to support GAMP 5, EudraLex Volume 4 Annex 11 (EU GMP Annex 11) and 21 CFR Part 11 compliance. Cybersecurity requirements are fulfilled according to standard IEC 81001-5-1.

The full overview of regulatory information including the intended purpose is part of the CliniMACS Plus Instrument user manual.

4.2 Data protection laws

When processing personal data with the CliniMACS Plus System, user discretion is strongly advised. The user is responsible for ensuring compliance with applicable data protection laws and regulations. According to the principles of privacy by design and default, Miltenyi Biotec has implemented security measures, especially the Defense-in-depth concept (see section 'Defense-in-depth concept for security').

4.3 Basic concept

The software running on the CliniMACS Plus Instrument includes core software and various application software (referred to as application process). The core software provides a common platform for all executable programs including application processes, tools, and settings (see Figure 4.1).

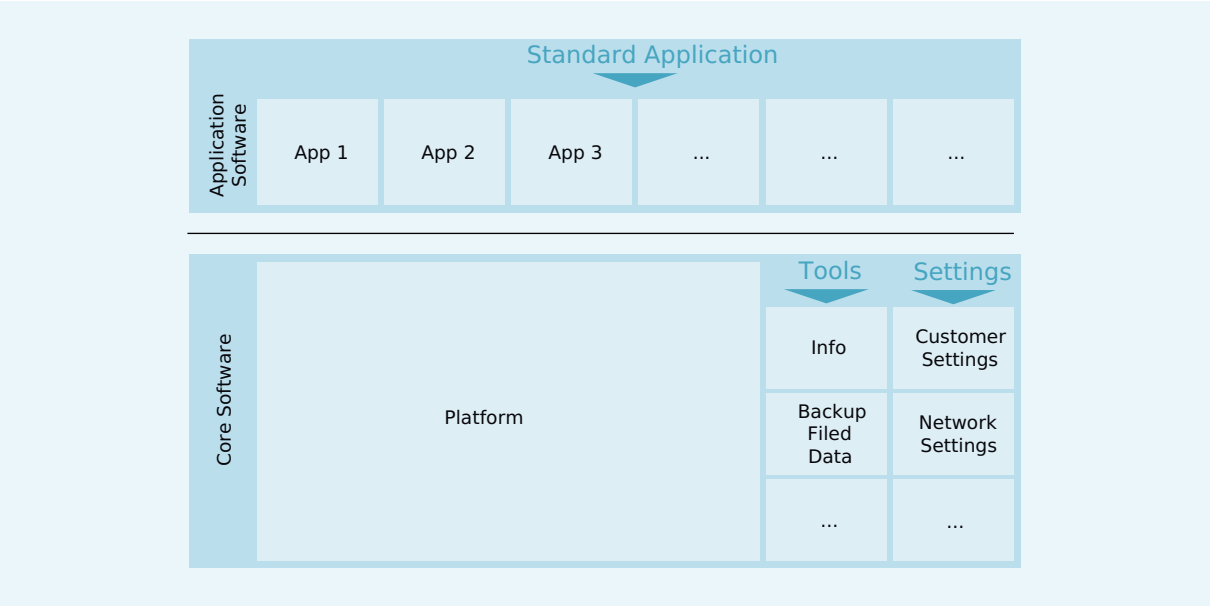


Figure 4.1: Overview of instrument software

The core software controls the instrument and execution of application processes and provides essential services as described in the following chapters and sections. The core software is also referred to as software within this user manual. The application software is executed by the core software and provides the application processes and user interfaces for the operation of the instrument. The core software and each application are independent entities allowing a separate update of a new application without changing the core software.

4.3.1 Application process

An application process is a standalone software that represents a biological process, for example the CD34 enrichment. This process is pre-validated, standardized, and provided by default. It contains a sequence of pre-defined hardware and software steps to automate the biological process. The user is guided step-by-step during the process.

4.3.2 Tool

A tool is an executable program, which can run a general purpose function outside an application process. For instance, check or change the status of the hardware, transfer data, shutdown of the instrument, etc.

4.3.3 Setting

A setting is an executable program to configure the instrument. For instance customer settings, network settings, and user management system (UMS) settings. For each executable program a separate log folder is created. The folder is named by '[Date]_[Time]_[SerialNumber]_[ExecutableProgram]'.

The content of this log folder is controlled by the executed program. For application processes, the customer-relevant log files are listed in Table 4.1.

IMPORTANT:
By using the file 'checksums.md5', it is possible to check if exported files are intact.

File/Folder name	Description	Format
Protocol.pdf	Electronic record of application run	.pdf
Protocol_Appendix_I.pdf	Error and warning log during application run	.pdf

Table 4.1: Log files of application processes

4.4 Graphical user interface

The GUI contains several sections: menu bar (with quick access menu), toolbar, status line, and content area (see Figure 4.2). During software operation, GUI elements and content change based on the activity and process.

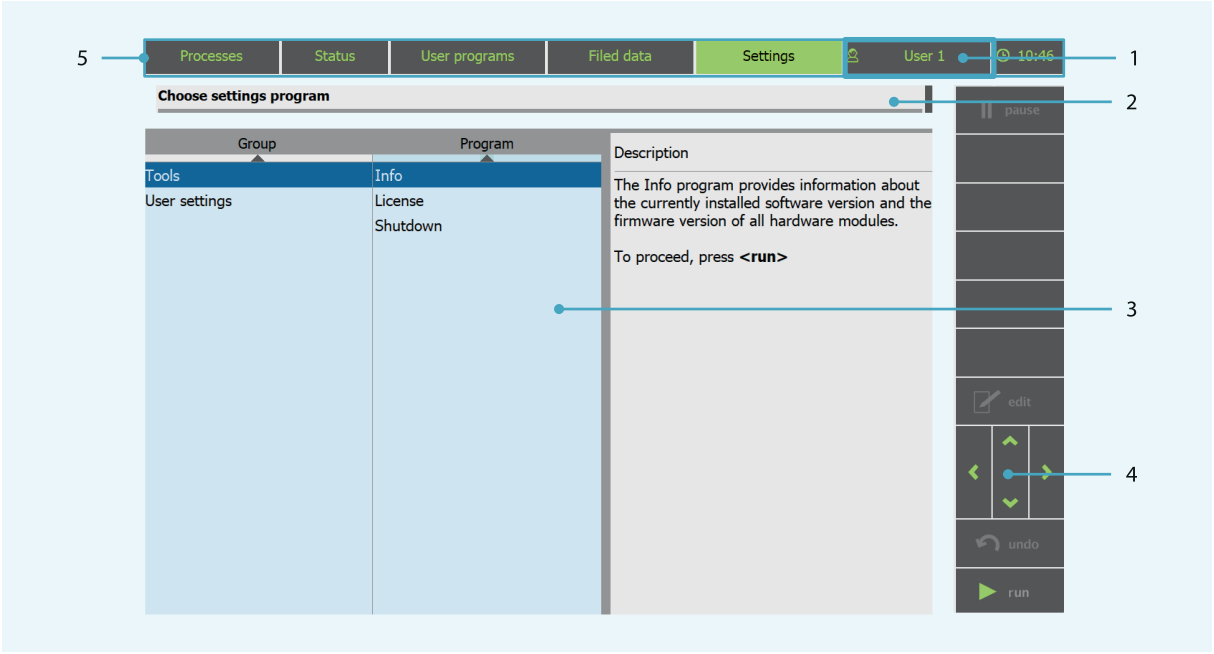


Figure 4.2: Sections of the graphical user interface

1 Quick access menu
2 Status line
3 Content area
4 Toolbar with navigation buttons
5 Menu bar

4.4.1 Menu bar and content area

The menu bar provides access to Processes, Status, User programs, Filed data, Settings, and the quick access menu. To activate a menu, tap in the respective area in the menu bar. A green background indicates the currently activated menu. The content area adapts according to the selected menu. Upon login, the Processes menu is selected by default and the list of processes is shown.

Menu	Description
Processes	Access to standard application processes installed on the instruments (see section 'Selecting an application process') and guides through the process run (see Figure 5.2)
Status	Access to instrument status during an application process run (see Figure 5.3)
User programs	Access to Miltenyi Biotec's custom user programs
Filed data	Access to filed data generated from processes, tools, and settings (see section 'Retrieving application logs')
Quick access menu	Access to logout, shutdown, and change password procedure, and, if respective role is assigned, to user management system, password policy, and audit trail
System time	Display of the current system time

Table 4.2: Menus in the menu bar

4.4.2 Status line

The status line (see Figure 4.2) contains brief information regarding the status of the current process.

4.4.3 Toolbar

The toolbar contains various buttons to control the process. The availability of the buttons and whether they are active or not, is controlled by the application process. Figure 4.3 shows example toolbars during two different application processes. A green color indicates an 'active' status, and a gray color indicates an 'inactive' status. Frequently used buttons are explained in Table 4.3.

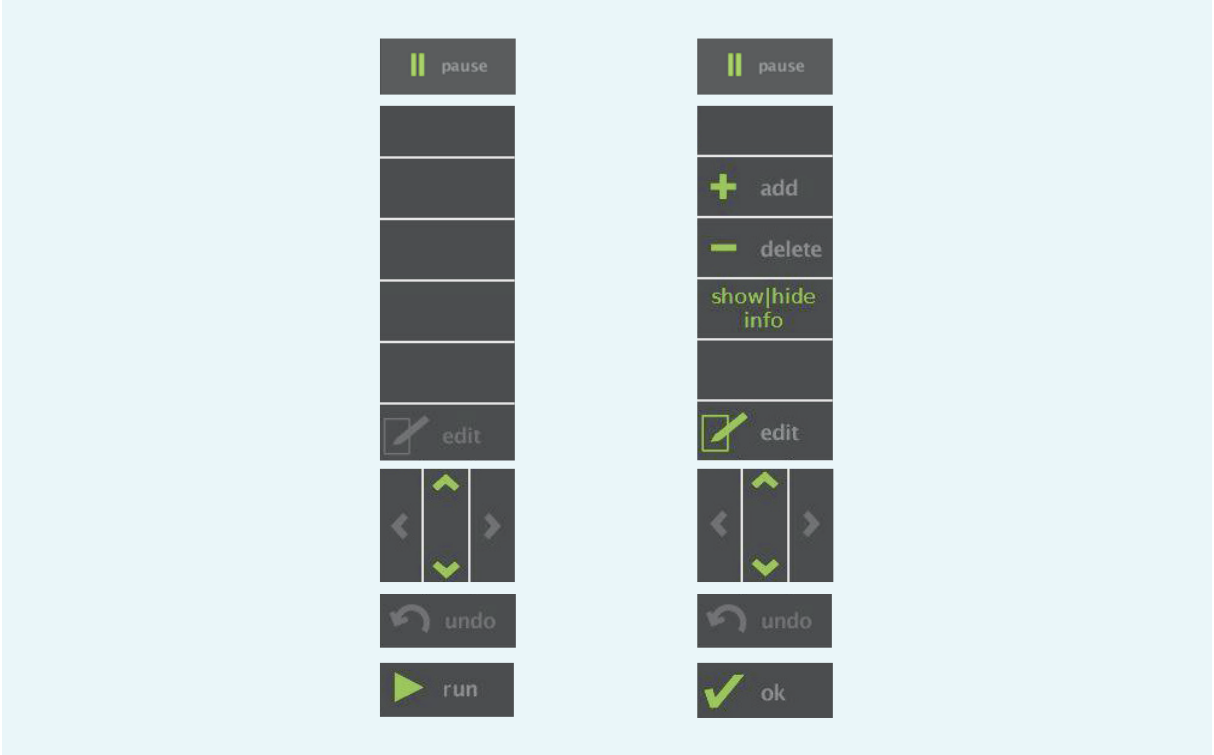


Figure 4.3: Dynamic and static buttons of the toolbar

Button	Description	Availability
pause	to temporary halt/suspend the currently running process	during a process run
edit	to activate the input field for manual data input (see section 'Input fields')	if input is possible
^ v	to select an element from a list (to move up and down in a list)	always
< >	to switch between lists	always
undo	to revoke one or more inputs to restore the original content of the screen	during a process run
run	to start a process, user program, or any other procedure	if a program is ready to be executed
ok	to confirm a selection or to close the active menu	always

Table 4.3: Frequently used buttons in the toolbar

4.4.4 Input fields

An input field represents a keypad and allows for the input of letters or numbers (see Figure 4.4). It can be opened by tapping edit in the toolbar.



Figure 4.4: The input field - keypad with letters

The following inputs are possible:

- To enter capital letters, tap ⌂
- To enter a space, tap SP
- To enter numbers, tap ?123
- To delete characters, tap ⌫

To confirm the input, tap ok at the bottom right of the input field. To close the input field without saving, tap × on the top right corner.

4.4.5 Pop-up windows

Pop-up windows might be shown while running executable programs. The running process is interrupted until the pop-up window is closed. If necessary, pop-up windows can be dragged around the screen while holding the top bar. There are different types of pop-up windows that can appear in various scenarios.

The pop-up window shows a gray background when input or confirmation is needed. Select one of the buttons to continue with the process.

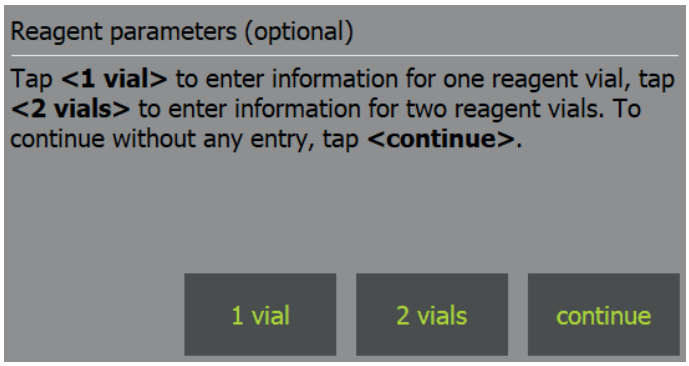


Figure 4.5: Gray pop-up window

The pop-up window shows an orange background when a warning occurred or an important decision needs to be confirmed. Select one of the buttons to make a decision.

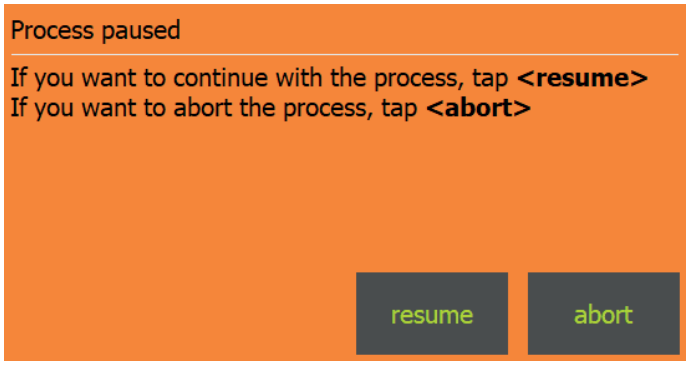


Figure 4.6: Orange pop-up window

The pop-up window shows a red background when an error occurred. Select one of the buttons to continue. If required, contact Miltenyi Biotec Technical Support.

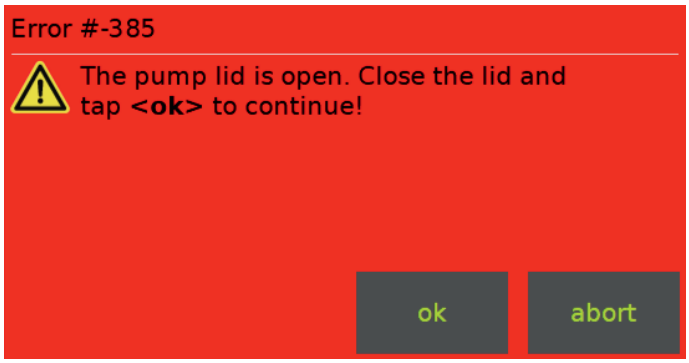


Figure 4.7: Red pop-up window

5

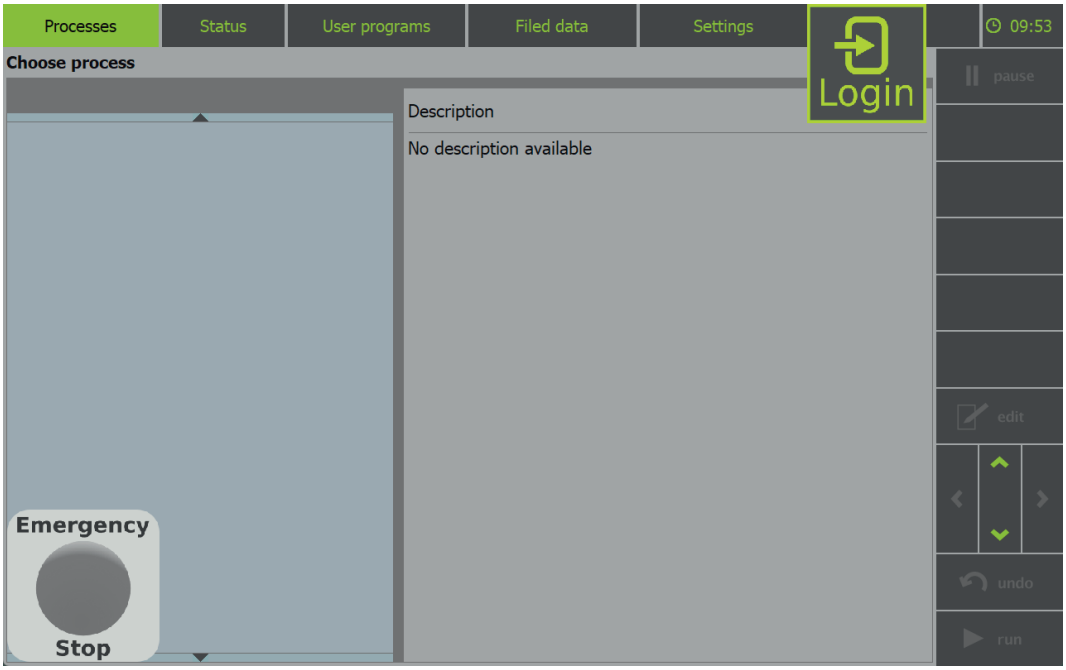
Basic operation

This chapter covers the basic operating functions of the CliniMACS Plus Instrument. These include switching on, logging in and out, shutting down, emergency stop procedures, application process controls, and viewing the instrument status.

5.1 Switching on the instrument

1. Plug the power cable of the instrument into a grounded electrical outlet.

2. Switch on the CliniMACS Plus with the power switch located on the rear side of the instrument.
   The start screen appears and shows the current software version. During the initialization, the instrument performs self-checking procedures. After the initialization process, a locked screen appears and only the **Login** button is active.



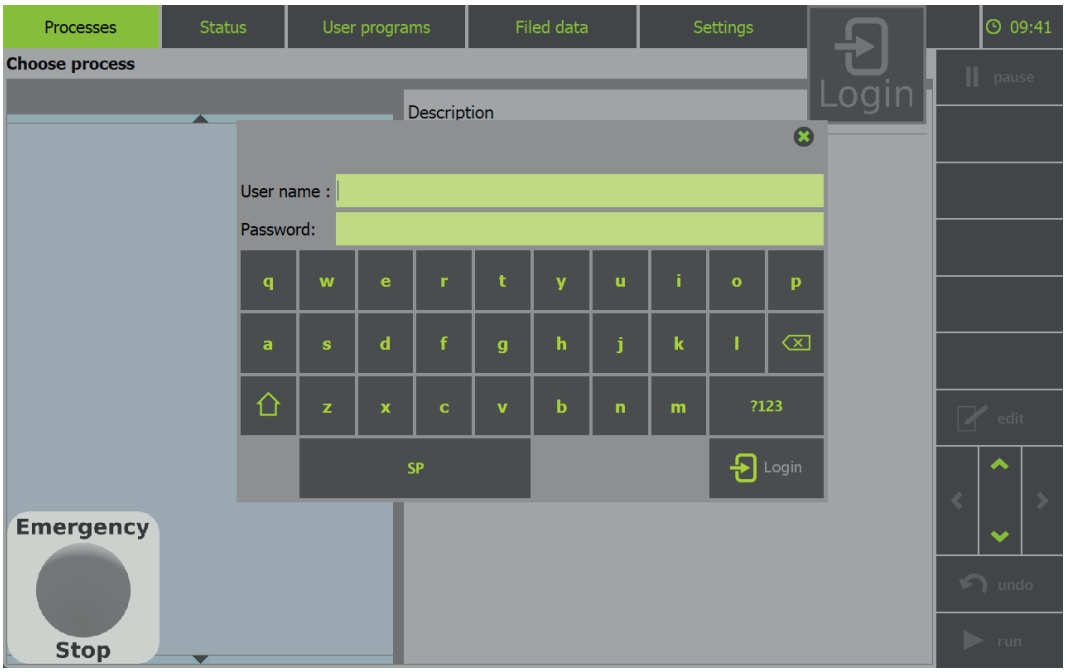
   If the instrument does not start up, switch off the instrument by using the power switch and disconnect it from the power supply. Check the power port. Then switch on the instrument again. If the instrument does not start correctly or the window shows an error message, note the error message number, switch off the instrument, and contact Miltenyi Biotec Technical Support.

5.2 Login

IMPORTANT:

- The username and password should be set up before login (see chapter 'User management' for details).
- Maxing out the login attempts locks the user completely. There is no option to reset the password, also not by Miltenyi Biotec Technical Support.
- In case of login failure, see section 'Login issues'.

1. To open the login window, tap **Login** in the upper right corner of the locked screen.
   A pop-up window appears, allowing the user to enter the user credentials:



2. Enter username and password and tap **Login** within the pop-up window.

5.3 Logout

IMPORTANT:
After 20 minutes (default) without interaction with the software, the user is logged out automatically.

1. Tap (**quick access menu**) and select **Logout** from the list.
2. To confirm the logout, tap **ok** in the pop-up window.

5.4 Shutting down the instrument

1. To shut down the instrument, choose one of the following options:
   - Tap (**quick access menu**) and select **Shutdown** from the list or
   - navigate to **Settings** > **Tools** > **Shutdown** and tap **run**.
2. In the pop-up window, confirm with **shutdown**.
3. Wait for the shutdown process to finish and switch off the instrument using the power switch located at the rear side of the instrument.

5.5 Emergency stop

An emergency stop pauses the currently running application or a tool in case of an emergency situation without login in advance. To meet the 21 CFR Part 11 requirements, a subsequent login and entering the reason of the emergency stop is required. The Emergency Stop button (see Figure 5.1) is only activated (indicated by the colors yellow and red) when an application or a tool is running and no user is logged in.

To resume the application, the user with the respective rights for the application needs to log in.

IMPORTANT:
The Emergency Stop button does not completely switch off the instrument, it has the same function as the pause button during a running application when a user is logged in.



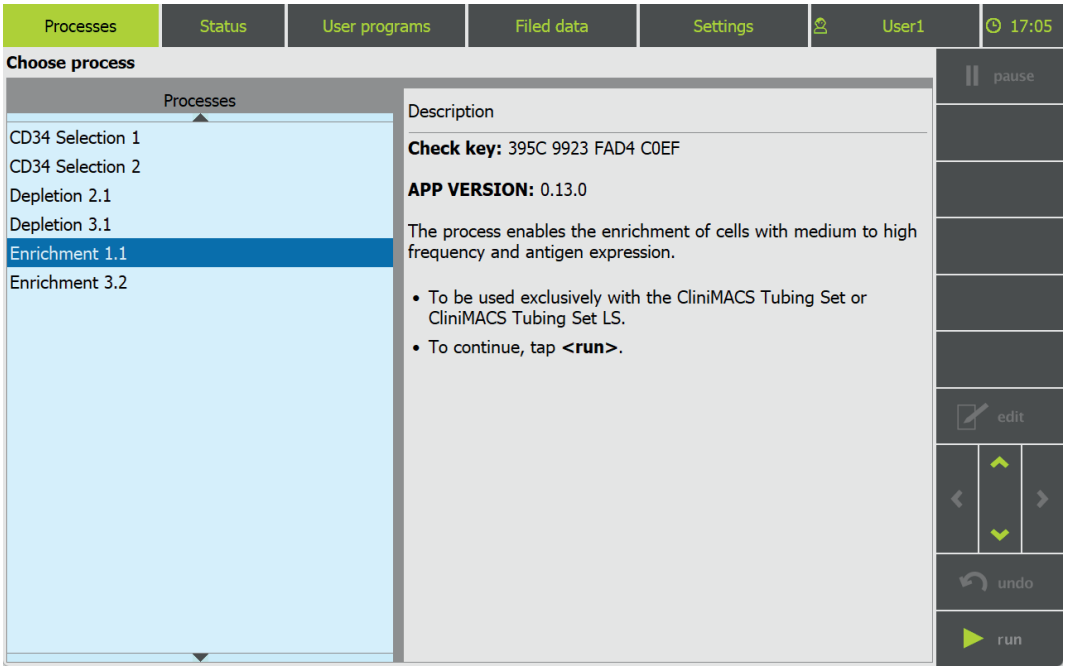
Figure 5.1: Emergency stop button

5.6 Selecting an application process

IMPORTANT:
The content in the process list adapts to the role and rights of the current user. An application is only shown if the currently logged-in user has access rights. For more information regarding user rights, see chapter 'User management' and section 'Roles and rights'.

1. Tap Processes in the menu bar for a standard application process. For a custom user program, tap User Programs.

2. To select the desired process from the process list, tap the application's name or use ^ and v on the toolbar to navigate through the available processes. A selected process is highlighted with a blue background. A description of the application can be found on the right.



5.7 Executing an application process

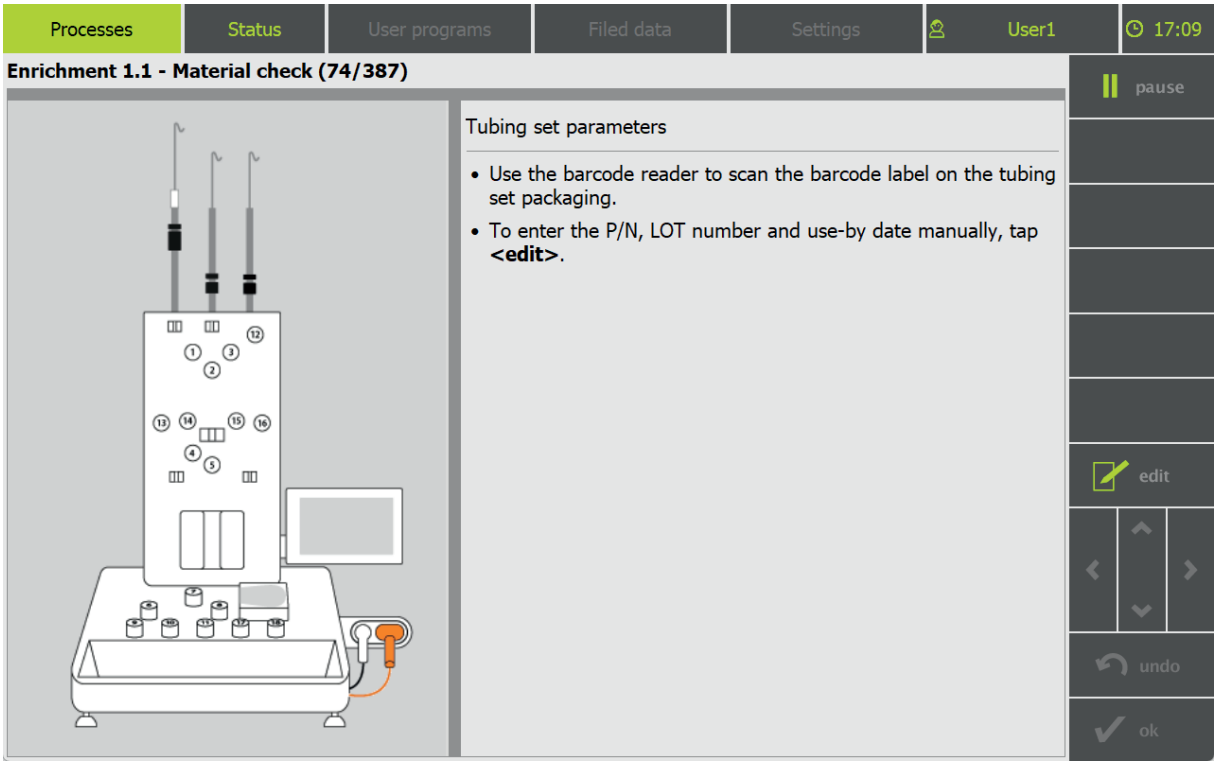


Figure 5.2: Exemplary step during the Enrichment 1.1 application

⚠ CAUTION

Risk of process failure due to failed login.

If login is not possible anymore, there is the risk of process failure.

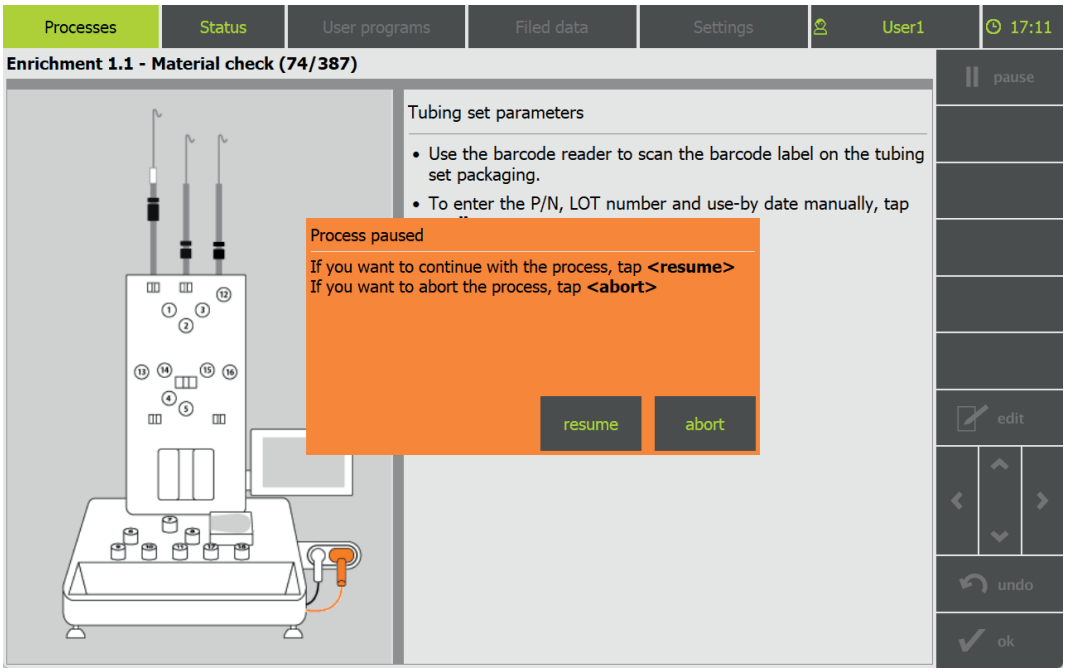
- Create appropriate user and administrator accounts with distinct passwords (see chapter 'User management') before initiating the start of an application on the instrument. In case an instrument login is not possible anymore, contact Miltenyi Biotec Technical Support.

1. To start a process, select the desired application and tap **run** in the toolbar.
   In some processing steps, user input is required. Typical required inputs are part number (P/N), LOT number and values of measurements. Part number and LOT number can be entered either with the barcode reader or manually. For manual entry or if barcode reader input is not accepted, the user can tap **edit** in the toolbar and use the input field.

2. When all required actions are completed, **ok** in the toolbar is enabled. To go to the next step, tap **ok**. To return to the previous step, tap **undo**.
   The software provides step-by-step guidance through the process. Figure 5.2 shows an example step of the Enrichment 1.1 application. The status line shows the current step name and index. The content area gives more information on the respective step. Follow the instructions in the content area for each step.

5.8 Pausing an application process

1. To pause the current process, tap **pause** in the toolbar.
   A pop-up window appears:



2. When a process is paused, the user has the following options to proceed:
   - To continue a paused process, tap **resume**.
   - To end the process, tap **abort**.

IMPORTANT:
An aborted process cannot be resumed.

5.9 Viewing the status of the instrument and of the application process

To check the operational state of the running process, tap **Status** in the menu bar (see Figure 5.3).

IMPORTANT:
Status information is only available during an application run. This page is blank when no application is running.

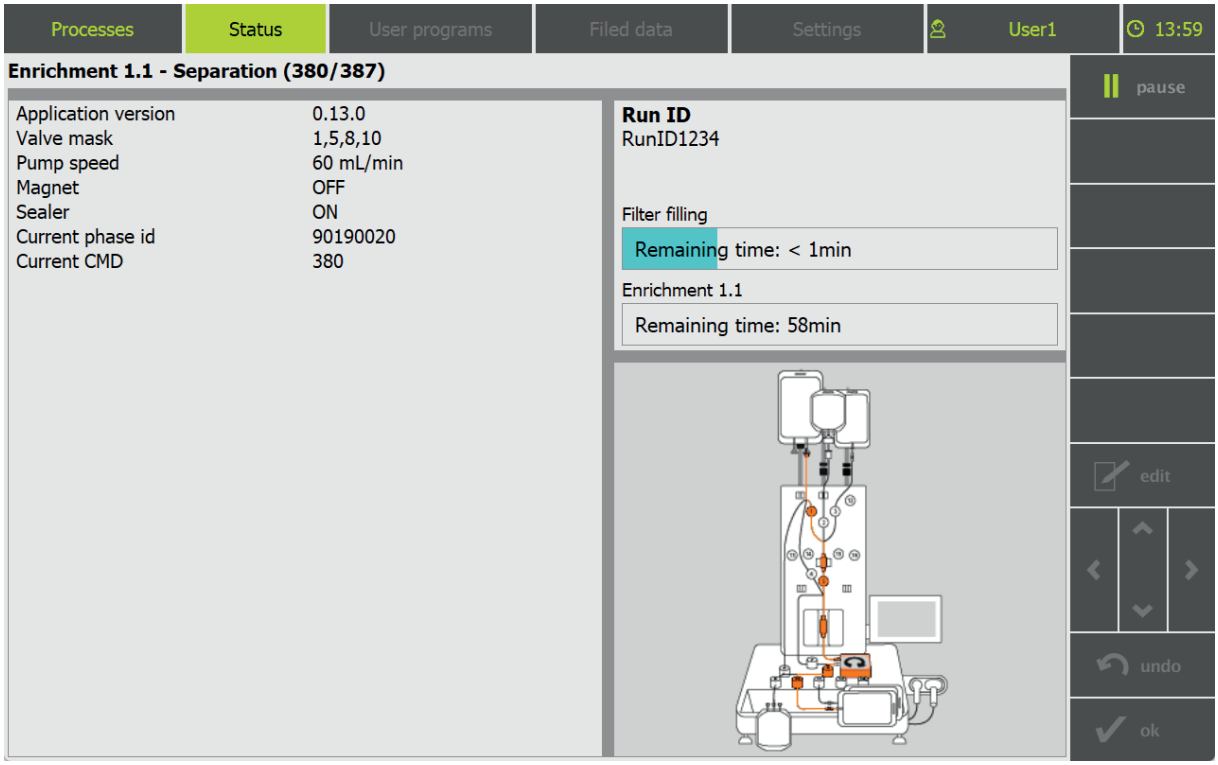


Figure 5.3: Exemplary overview of instrument status and application process status

The content area shows the following elements:

- Process-related parameters (see Figure 5.3, left): a list of all relevant process parameters
- Info box and progress status (see Figure 5.3, top right): process-related information, for example run ID, progress of subprocess/process, and remaining time before next user interaction
- Graphical overview (see Figure 5.3, lower right): graphical representation of the running subprocess

6

Data access

This chapter describes how to access the data recorded by the instrument. It describes how to retrieve application logs by using a USB flash drive or the file sharing option and how to retrieve audit trail information.

6.1 Retrieving application logs

6.1.1 Viewing and exporting log files to USB flash drive

The **Filed data** menu shows the log files generated from the application processes, tools, and settings. In the content area, the file list shows the time, name, type, duration, and status of the process run.

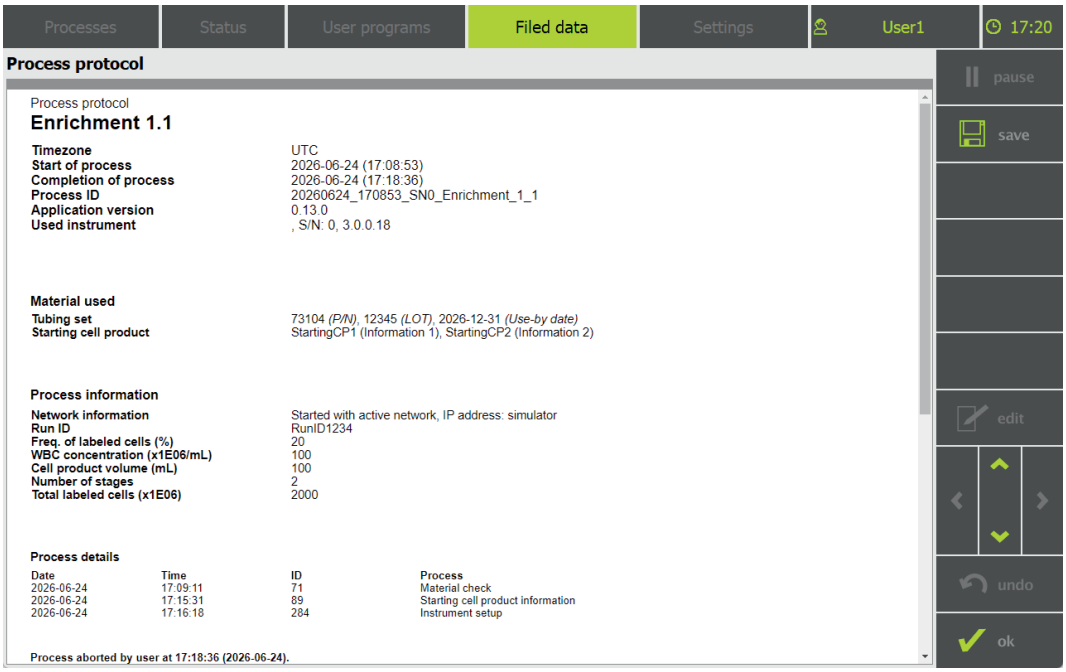
IMPORTANT:
The **Filed data** menu is not available during a process run. The respective touch button is inactive.

Viewing log files

1. To view the content of the process protocol PDF and protocol appendix PDF, select the target log and tap ok.



The content of the selected file is shown in the content area:



2. To return to the list of log files, tap ok.

Exporting log files to a USB flash drive

1. Insert a USB flash drive.

2. Open the target log file and tap save in the toolbar.

IMPORTANT:

- Make sure that the name of the USB flash drive is not 'netext' as this term is reserved for the software.
- To backup all process data, the Backup Filed Data tool can be used, see section 'Backup filed data'.
- Only USB flash drives formatted as FAT32 are supported. The USB flash drive should not be password-protected.

6.1.2 Retrieving files via file sharing

The log files generated during the application process can be retrieved via a shared network folder. Once the application process is complete, all generated files will be automatically placed in a subfolder created for each instrument within the shared folder. Figure 6.1 shows the file structure in the shared folder. To enable file sharing, configuration is required. To setup file sharing, follow the instructions in section 'Connecting to a network drive'.

IMPORTANT:
Log files stored on the instrument are protected by access control to ensure that only authorized personnel have access. Once these files are transferred to a network drive, it becomes the user's responsibility to implement appropriate access control measures.

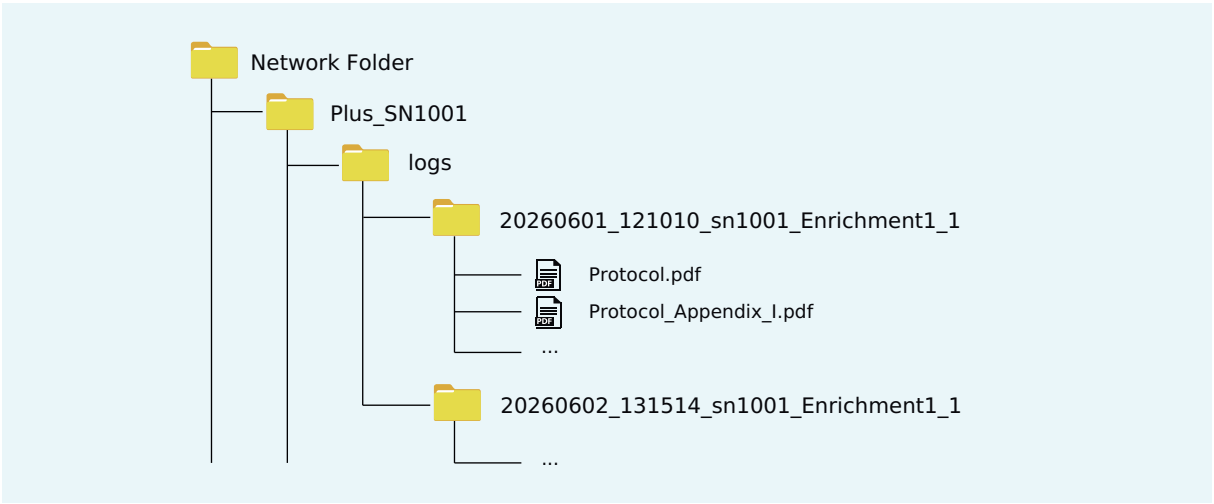


Figure 6.1: File structure in the shared network folder (exemplary)

6.2 Retrieving audit trail

The audit trail system records all the user interactions with the software. Each user interaction results in an audit trail record with executed user, timestamp, and description of the interaction. The audit trail can be exported in '.pdf' and '.csv' format. Table 6.1 shows the audit trail format.

Time	Category	Type	User	Description
2020-Jul-21 10:33:44	User interaction	Pop-up close	AccountID	Progress paused 'warning'
...	...	...	...	...

Table 6.1: Audit trail format

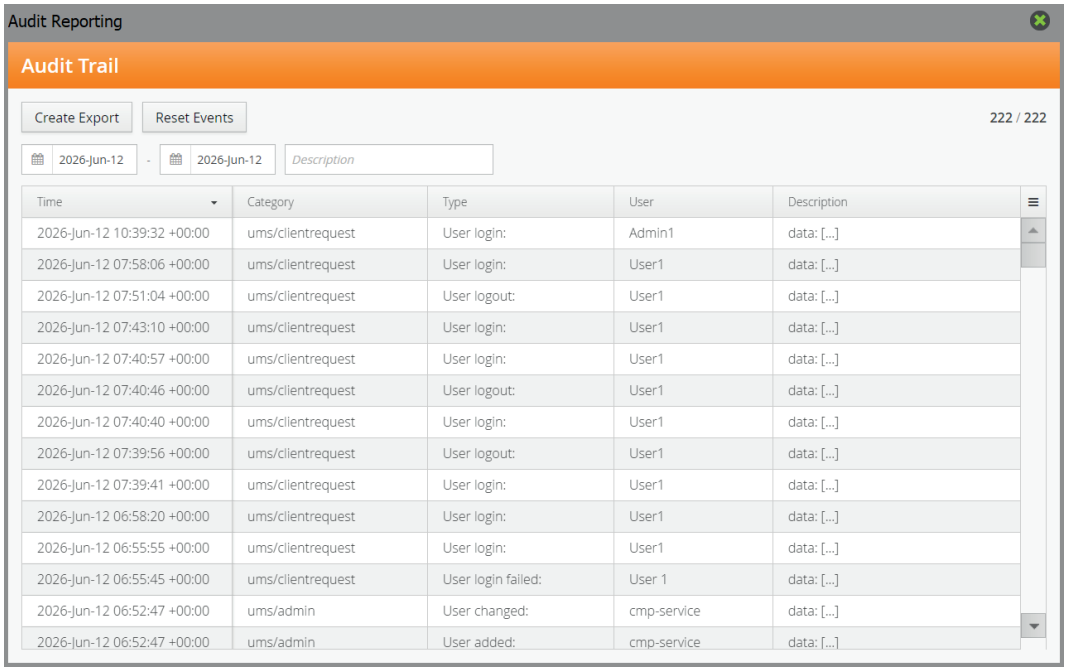
IMPORTANT:

- The timestamp of the audit trail record is always UTC time
- An 'ATS User' role or a role with 'Audit Trail Management' rights is needed to access the audit trail system
- An 'ATS User' role has full access, which allows viewing, exporting, and deleting audit trail records
- A new role can be created for limited access to audit trail functions. See chapter 'User management' for more details on how to configure roles and rights

6.2.1 Viewing audit trail

To open the Audit trail, go to > **Audit Reporting**.

The **Audit Trail** menu contains a list of all available audit trail events on the instrument:

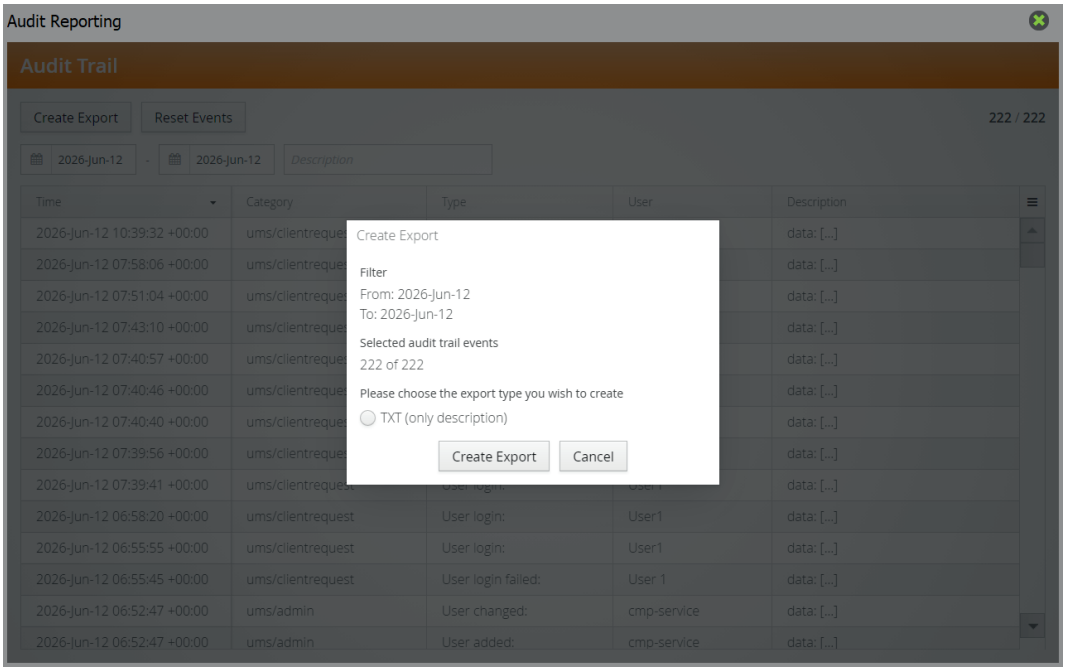


6.2.2 Exporting audit trail

1. Enter the filter criteria (start date, end date, and description) in the fields of the **Audit Trail** menu. If no criteria is entered, all audit trail records are exported.

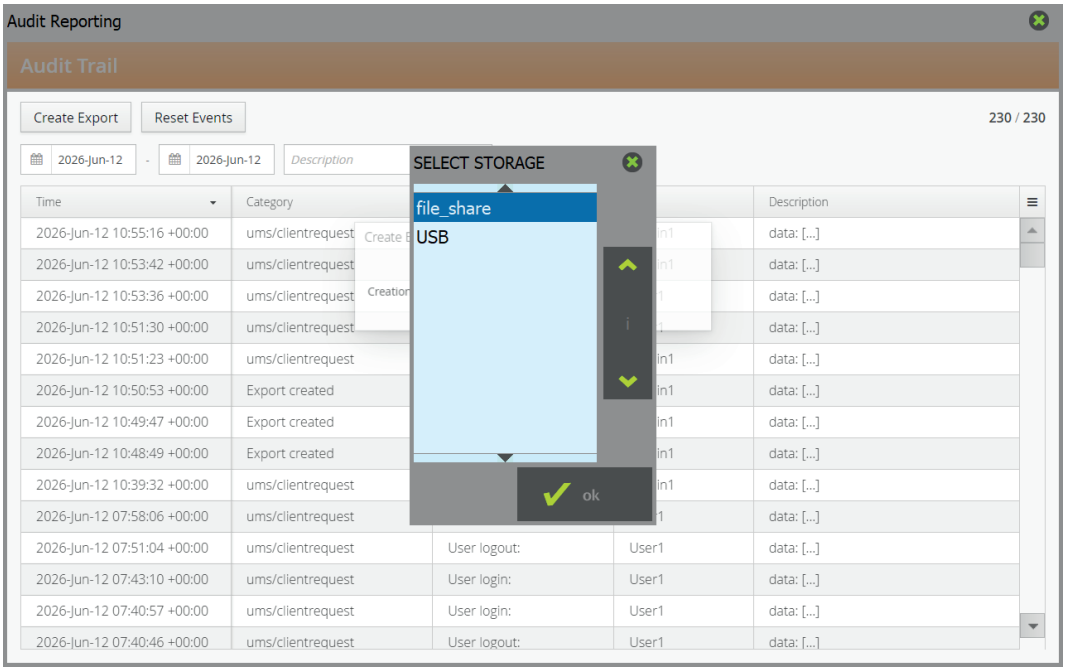
2. Tap **Create Export** above the filter criteria.

   A pop-up window is shown:



3. Choose the format and tap **Create Export** in the pop-up window.

4. If multiple storage locations are detected, for example file sharing is configured and a USB flash drive is inserted, the storage location needs to be chosen:



5. Wait until the process is completed and check whether the file has been exported.

6.2.3 Deleting audit trail

IMPORTANT:

- Deleted data cannot be restored.
- Make sure only authorized users have the right to delete audit trail data. To configure roles and rights, see chapter 'User management'.
- It is not possible to delete single entries.

1. To delete all audit trail entries, tap **Reset Events**.

2. Confirm with **Continue Reset**.
   After the reset, all records are deleted. A new record for the delete action is added.

7

Tools and user settings

This chapter describes software tools and user settings and how to access them.

7.1 Accessing tools and user settings

Two types of programs can be found in the **Settings** menu: **Tools** and **User settings**.

IMPORTANT:
The available tools depend on the user's role. Tools and user settings are not available during a process run.

To select and run a tool or user setting, proceed as follows:

1. Navigate to the **Settings** menu and select **Tools** or **User settings** from the list.
2. Tap on the desired program from the program list or use the navigation buttons to browse and select the program. The selected program is highlighted with a blue background. Detailed information about the selected tool or user setting can be found in the description field.
3. To start the selected program, tap **run** in the toolbar.

7.2 Tools

All tools (see Figure 7.1) can be found in **Settings** > **Tools**.

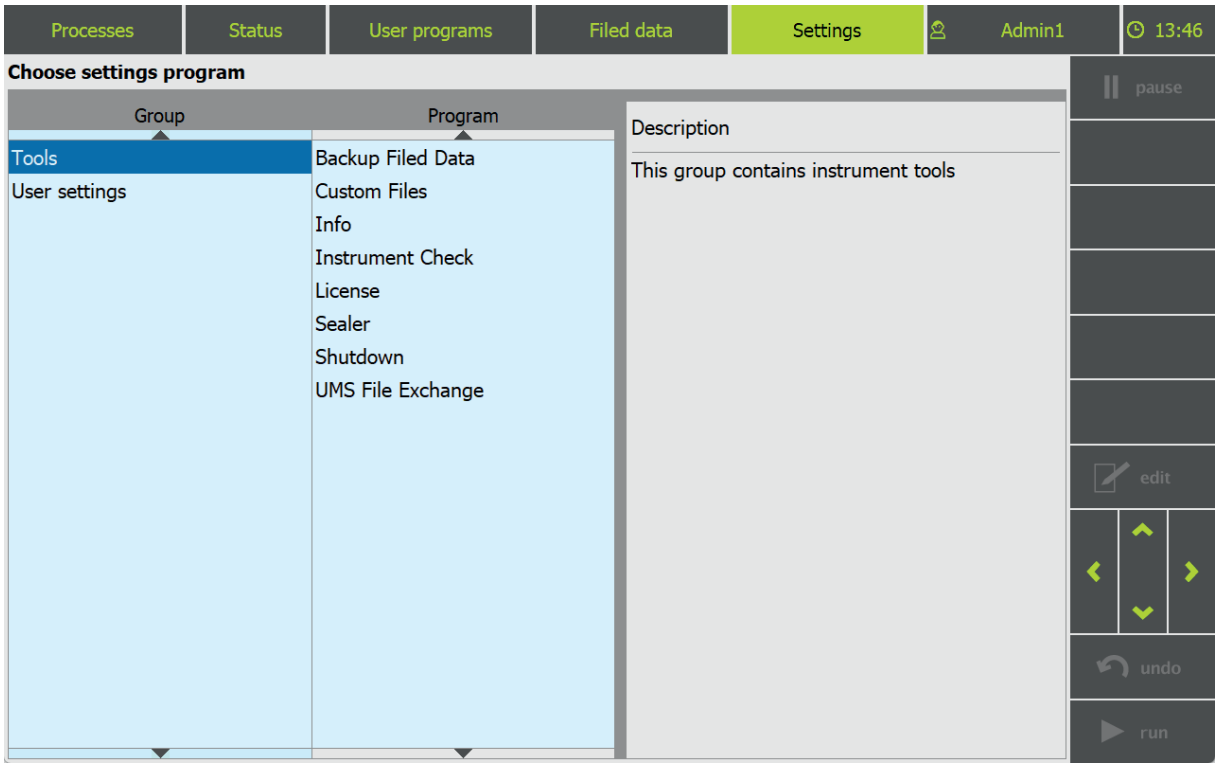


Figure 7.1: Tools menu

7.2.1 Backup filed data

The Backup Filed Data tool can be used to copy all process data to a backup location or to delete all process data.

IMPORTANT:

- If file sharing is configured and enabled, files can also be exported to the file sharing folder (see section 'Connecting to a network drive').
- It is recommended to backup the process data regularly and then delete it from the instrument. Otherwise, a user prompt message may pop up stating that the program must not be started because the limitation for filed data has been reached.
- If using a USB flash drive for backup, the USB flash drive must be formatted as FAT32 and should not be password-protected.

Backup process data

1. To backup process data, insert a USB flash drive.

2. Go to **Settings** > **Tools** > **Backup filed data** and tap **run**.

3. To start copying the data, tap **Backup** on the prompt.

4. Wait until copying is finished and then tap **ok**.
   Data has been saved. Verify that the files have been downloaded completely.

Delete process data

1. To delete process data, go to **Settings** > **Tools** > **Backup filed data** and tap **run**.

IMPORTANT:
Only delete data when it is no longer needed. Deleted data cannot be recovered.

2. Tap **Delete**.

3. To start deleting the data, confirm with **yes** on the prompt.

4. Wait until deletion is finished and then tap **ok**.
   After deletion all records from **Filed data** are deleted. One record for executing the Backup filed data tool is created.

7.2.2 Custom files

This program is used to temporarily add new applications to the instrument via USB flash drive.

7.2.3 Info

This tool provides detailed information regarding software and hardware components. Important information includes:

- Serial number
- Software version and build number
- Hard drive space usage, including remaining space, used space, and total space
- Network information (hostname, IP address, and MAC address)
- Runtime duration (including all applications and tools) and idle time (time the instrument was not running an application)
- Module information

7.2.4 Instrument check

This tool performs a semi-automated check (user interaction is still required) of the backplane connector, the LED signal lamp, the magnetic separation unit, the peristaltic pump, and the pinch valves.

7.2.5 License

This tool shows the license information of all software packages and libraries used by the operating system and the instrument software (including applications).

7.2.6 Sealer

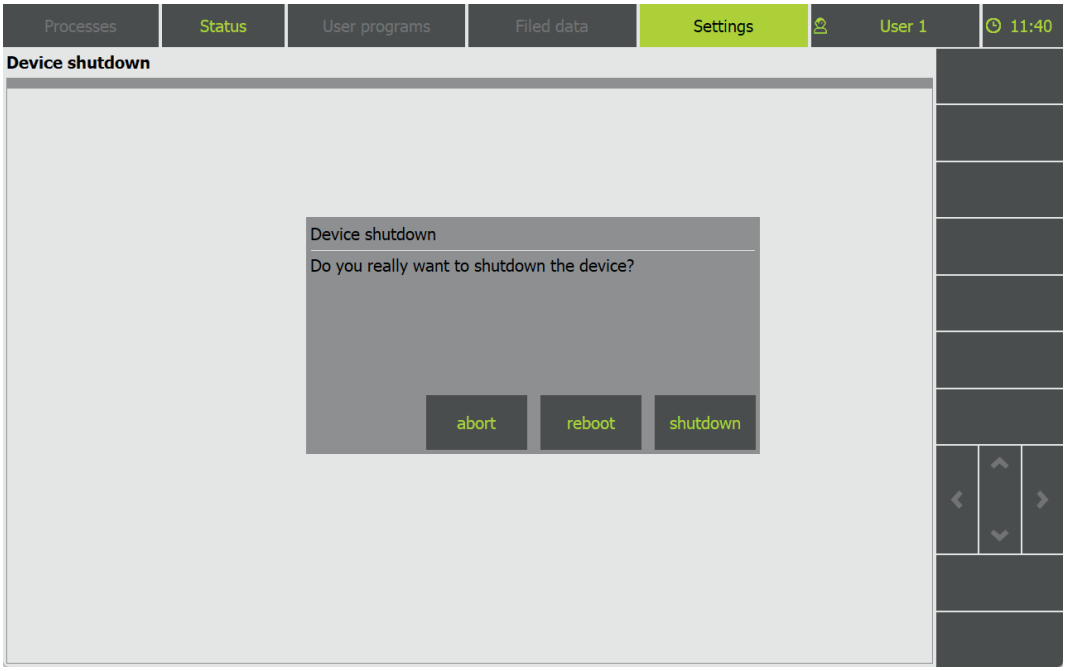
This tool is used to turn on or off the MACS® TubeSealer and to show its current state.

7.2.7 Shutdown

This tool prepares the shutdown sequence of the instrument. The user can reboot or shut down the instrument.

1. To execute the shutdown tool, choose the tool and tap **run** in the toolbar.

2. Select **abort**, **reboot**, or **shutdown** and wait until the process is finished.



7.2.8 UMS file exchange

The UMS file exchange tool can be used to transfer UMS configuration files and SSL certificate files.

7.3 User settings

All settings (see Figure 7.2) can be found in **Settings** > **User settings**.

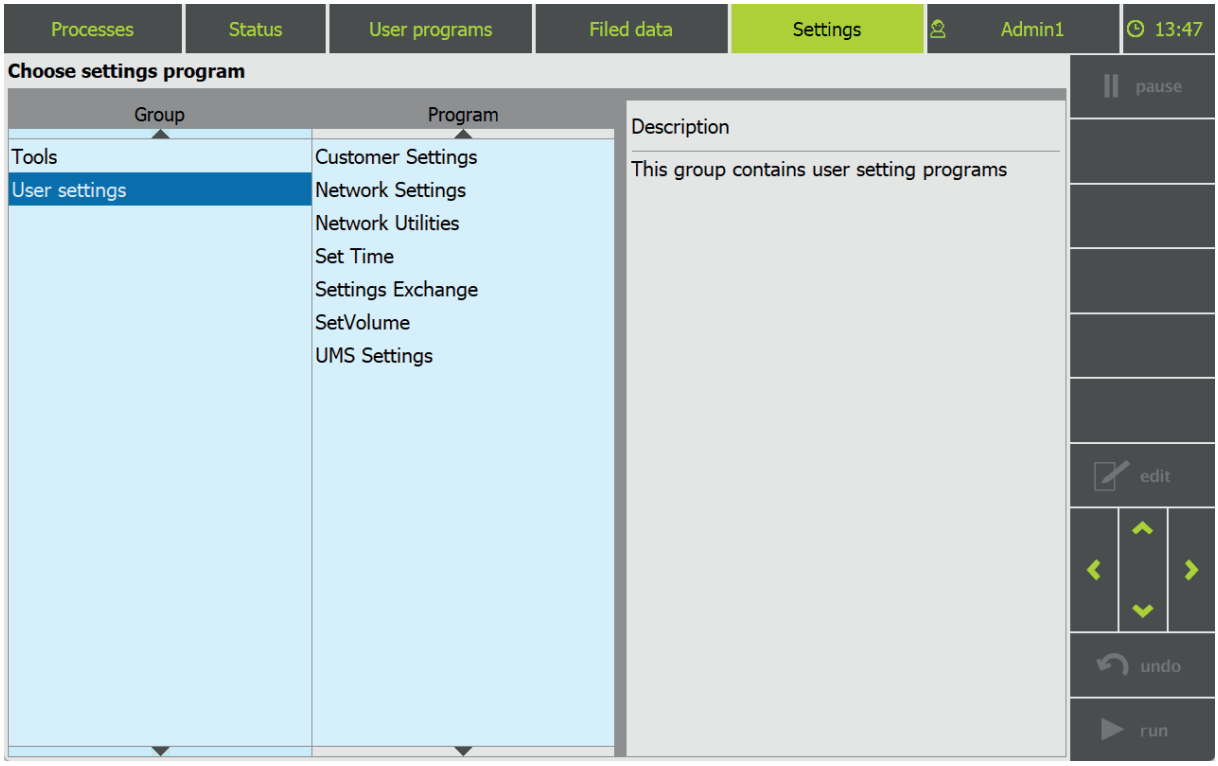


Figure 7.2: User settings menu

7.3.1 Customer settings

Customer settings are general settings for the instrument, including language, company name, department, street, postal code, city, instrument name, contact person, location, and email notification. The latter is described in more detail in section 'Connecting to an email server'.

7.3.2 Network settings

Under network settings the user can set all required information regarding network integration of the instrument. For a detailed explanation, refer to the following sections:

- 'Connecting to a local network' for network integration
- 'Connecting to an LDAP server' for Lightweight Directory Access Protocol (LDAP) connection
- 'Connecting to a network drive' for file sharing
- 'Connecting to an email server' for the set up of email notifications
- 'Enabling network time synchronization' for network time synchronization

7.3.3 Network utilities

The network utilities are used to execute network-related console commands.

7.3.4 Set time

This function allows to set the date and time on the instrument.

IMPORTANT:
The time set using this tool is automatically overwritten if Network Time Synchronization is enabled. To set up Network Time Synchronization, see section 'Enabling network time synchronization'.

7.3.5 Settings exchange

The **Settings Exchange** tool enables copying settings to different instruments. These settings include customer settings, module settings, and network settings and are copied in two steps:

- Export settings from the instrument to a USB flash drive
- Import settings from the USB flash drive to another instrument

IMPORTANT:

- If file sharing is configured (see section 'Connecting to a network drive'), files can also be exported to the file sharing folder.
- If using a USB flash drive for importing or exporting, the USB flash drive must be formatted as FAT32 and should not be password-protected.

Export settings to USB flash drive

1. Insert a USB flash drive.
2. Go to **Settings** > **User settings** > **Settings Exchange** and tap **run**.
3. Tap **export**.
4. Check the values on the screen. To proceed, tap **continue** in the toolbar.
5. Enter a password to protect the exported settings and tap **ok**.
6. Enter the password a second time and tap **ok**.

7. Wait until the export is successful. To close the tool, tap **ok**.

Import settings from USB flash drive

1. Insert a USB flash drive with the desired user settings file.
2. Go to **Settings** > **User settings** > **Settings Exchange** and tap **run**.
3. Select **Import**.
4. Select the file to be imported and tap **ok**.
5. Enter the password that protects the settings and tap **ok**.
6. Check the values on the screen. To proceed, tap **continue** in the toolbar. To abort, tap **pause**.
7. To confirm the pop-up window indicating a required restart, tap **ok**. To close the tool, tap **ok** again.

7.3.6 SetVolume

This program sets the volume of the instrument's speaker.

IMPORTANT:
It is not possible to enter a volume below 50%.

7.3.7 UMS settings

This program manages general UMS settings, except for UMS network settings. The latter are described in more detail in chapters 'Network integration' and 'User management'.

8

Network integration

This chapter describes the enabling of network time synchronization and different options of network integrations. It comprises the connection to a local network, to an LDAP server, to a network drive, and to an email server.

The instrument can be connected to a local area network (LAN) using a USB-ethernet adapter. An appropriate network integration is needed to use the following functions:

- Centralized user management (that is LDAP)
- Automatic file sharing
- Email notification
- Network time synchronization

To use the above mentioned functions, first connect the instrument to the local network (see section 'Connecting to a local network'). Then follow the instructions for the specific functions.

IMPORTANT:

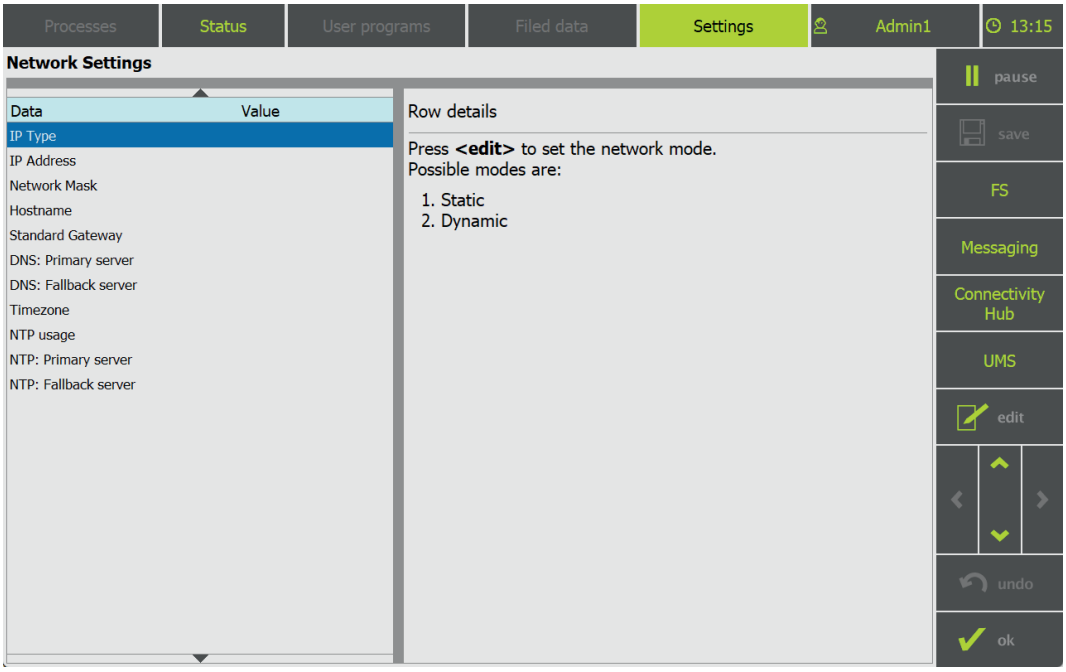
- Only UMS users with the administrator role 'Administration tools user' or users with 'Network Setting' rights have access to this setting. To configure rights and roles, see chapter 'User management'.
- The **Connectivity Hub** button may be shown on the screen, however, it is currently disabled and will remain so until this function is supported.
- The user must ensure that the firewall settings allow data exchange between the instrument and the desired server/client. The customer is responsible for the configuration of firewall settings.
- Some setting changes require a reboot of the instrument to be effective.

8.1 Connecting to a local network

IMPORTANT:
If network ports in your organization are secured by MAC address filters, contact your local IT service provider for proper setup.

1. Connect the instrument with the local network using a USB-ethernet adapter.

2. To enter the network settings, go to **Settings** > **User settings** > **Network Settings** and tap **run**.
   The 'Network Settings' menu appears.



3. To choose between static IP address and dynamic IP address, select **IP Type** from the list. Tap **edit** in the toolbar and enter the desired value in the input field.

Static IP

1. Select **IP Address** in the list, tap **edit** in the toolbar and enter the IP address in the input field.
2. Select **Network Mask** in the list, tap **edit** and enter the network mask in the input field.
3. To enter the name of the instrument, select **Hostname** and tap **edit**.
4. To enter IP address of the gateway, select **Standard Gateway** and tap **edit**.
5. Optional: To choose the time zone, select **Timezone** and tap **edit**. Default time zone of the instrument is Coordinated Universal Time (UTC).
6. Verify that the instrument is connected to the local network.

Dynamic IP

1. To enter the name of the instrument, select **Hostname** and tap **edit**.
2. The dynamic server must be configured. Enter an IP address for the primary and the fallback server.
3. Optional: To choose the time zone, select **Timezone** and tap **edit**. Default time zone of the instrument is UTC.
4. Verify that the instrument is connected to the local network.

8.2 Connecting to an LDAP server

To configure the connection to the LDAP server, go to the (quick access menu) and select **User Management**. In the **User Management** menu select **Configuration** > **LDAP Configuration**. To configure LDAP, follow the steps in Figure 8.1.

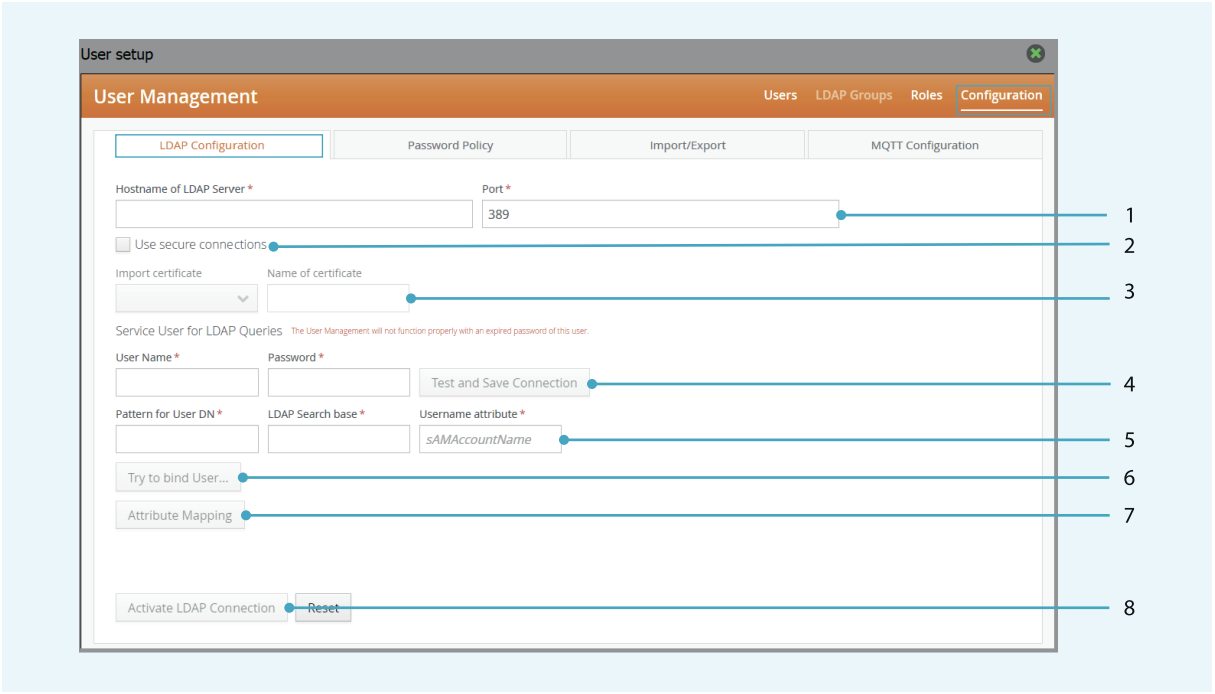


Figure 8.1: Required steps to configure LDAP in the user management menu

1. Enter the hostname and the IP address of the LDAP server.

2. Select a secure connection if required. This will automatically set the port from the standard value 389 to port 636 for a secure LDAP connection. For a secure connection, follow the instruction in section 'Importing user management settings' to import the certificate to the instrument.

3. To import certificates, select the certificate in the **import certificate** dropdown list.

4. Enter the username and password of a valid LDAP account using the full LDAP path of the username. Tap **Test and Save Connection**. A pop-up appears indicating that the connection is successful.

5. Enter the pattern, search base, and username attribute. The pattern for user domain name should contain the full path. These entries are dependent on user LDAP organizational structure and domain name. To show a brief explanation and examples of typical values, hover over the textboxes. It might help to have someone with access to an LDAP browser program to show the organizational units on there.

   Typical values are as follows:
   - Pattern = '<domain>\{0}', for example 'customername_dev\{0}'
   - Search base = 'OU=organization,DC=customername'
   - Username attribute = 'sAMAccountName'

6. Tap **Try to bind User...**. In the pop-up window, enter a valid username (the username can be the same username used for the login test). To continue, tap **Bind User in Searchbase**. If successful, the Account ID pop-up closes. Otherwise, an error message is shown.

7. Tap **Attribute Mapping**. In the pop-up window, the previously entered username attribute is automatically mapped to the 'User Name' field. Enter the same value for 'initials' as for 'User Name'. Entering values here will automatically fill out some information when a user is created. To return to the LDAP configuration page, tap **save**.

   IMPORTANT:
   It is necessary to enter initials since this value is considered mandatory information for users of the CliniMACS Plus Instrument. Missing or improper configuration of the attribute map may cause login failure.

8. Tap **Activate LDAP Connection**. Note that this button is only active if the previous steps were successful.

By following these steps (see Figure 8.1), the LDAP connection is fully configured and can be used to create LDAP groups and LDAP users in the **User Management**. For further details on managing accounts and roles, refer to chapter 'User management'.

8.3 Connecting to a network drive

After the application process finishes, the automatic file sharing immediately transfer all log files to the network drive. The audit trail records can also be exported to the network drive manually triggered by the user (see section 'Exporting audit trail'). The automatic file transfer is implemented based on the SMB protocol. The supported versions of SMB protocol include SMB 1.0, SMB 2.1, and SMB 3.0 (default).

IMPORTANT:
Server Message Block (SMB) 2.0 and SMB 3.0 is recommended. SMB 1.0 is only supported for legacy reasons, and should only be used for interacting with legacy equipment.

Prerequisites:

- Make sure the SMB server is reachable. Check the SMB protocol version of the server before starting.
- Create a folder on the SMB server for data storage. Note down the share name. This can be an anonymous share (accessible for guest account) or authenticated share (accessible for only to specified account).

  IMPORTANT:
  Authenticated share is recommended for data security.

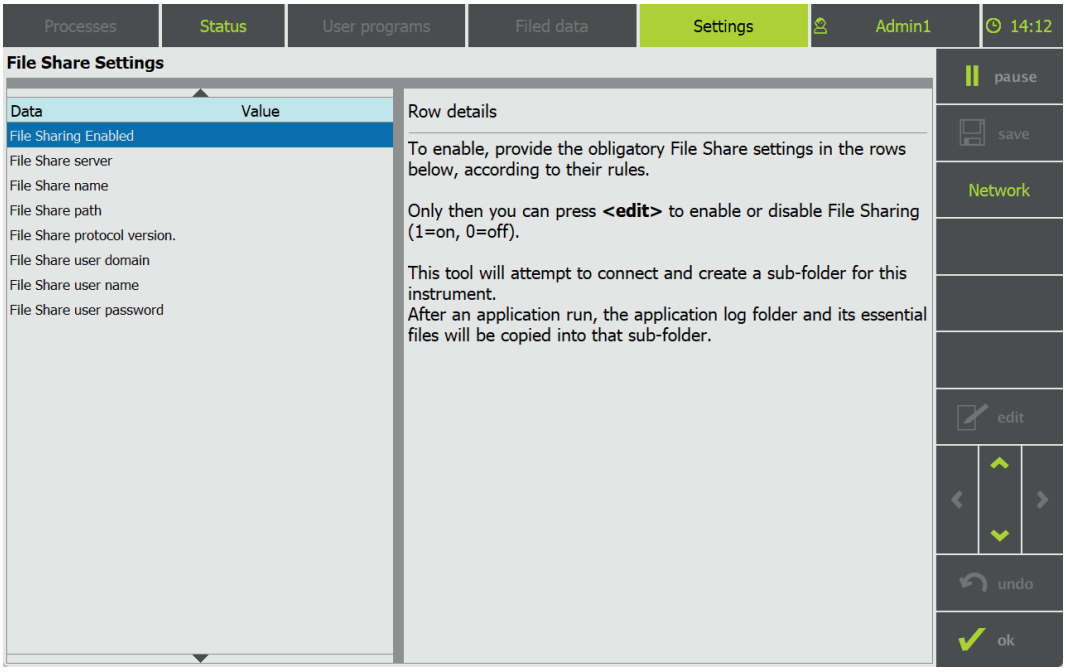
- If using authenticated share, a password-protected account is required. This account should have read and write access to the share folder on the SMB server.
- Connect the instrument to Ethernet and enable the network.

IMPORTANT:
It is important to enter all file sharing parameters before enabling the file sharing option, as any subsequent changes will disable file sharing. After configuring the settings, the instrument must be rebooted to complete the setup. Changes to the file transfer configuration are applied during reboot.

1. To enter the **Network Settings**, go to **Settings** > **User settings** > **Network Settings** and tap **run**.

2. To open the File Share Settings, tap FS in the toolbar.

   The File Share Settings menu appears:



3. To enter the hostname or IP address of the SMB server, select File Share server and tap edit.

4. To enter the Share Name, select File Share name and tap edit.

5. Optional: Select File Share path and tap edit to enter a file path.
   - If a path is entered, the instrument-generated files are pushed to '\\[File Share server]\[File Share name]\[File Share path]\'.
   - If the path is empty, the generated files are pushed to '\\[File Share server]\[File Share name]\'.

IMPORTANT:

Do not use spaces in the File Share path. If the folder is not found, the software gives a warning.

6. To enter the SMB protocol version, select File Share protocol version and tap edit.

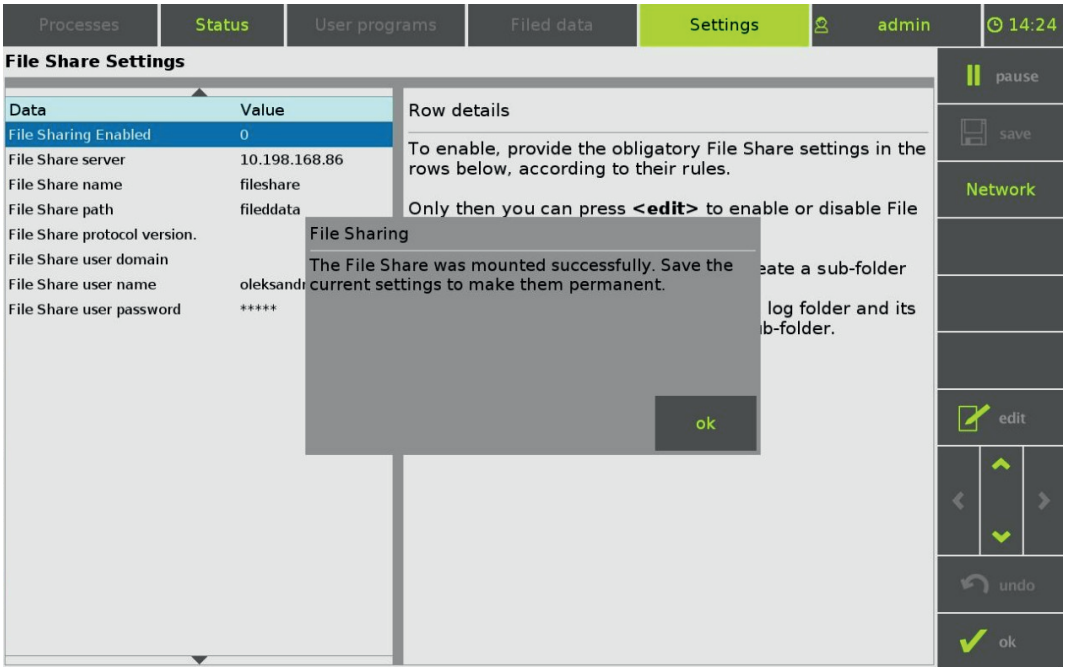
7. To enter the user domain, select File Share user domain and tap edit. Repeat the steps for File Share user name and File Share user password.

IMPORTANT:

If 'Guest' user is used to share the storage folder, File Share user domain, File Share user name and File Share user password must be empty.

8. Set File Sharing Enabled to 1.

After configuration, a pop-up shows the success of configuration:



IMPORTANT:
Modifications of file sharing parameters disable file sharing and it needs to be re-enabled manually. Always confirm that file sharing is enabled by setting the value of 'File Sharing Enabled' to '1' after changing any parameter.

8.4 Connecting to an email server

The software can send out an email to a defined email address in case of error or warning messages during a process run. The email contains the error or warning message and a screenshot of the instrument (see Figure 8.2). The email notification supports Simple Mail Transfer Protocol (SMTP) and the secure version of SMTP (SMTPS).

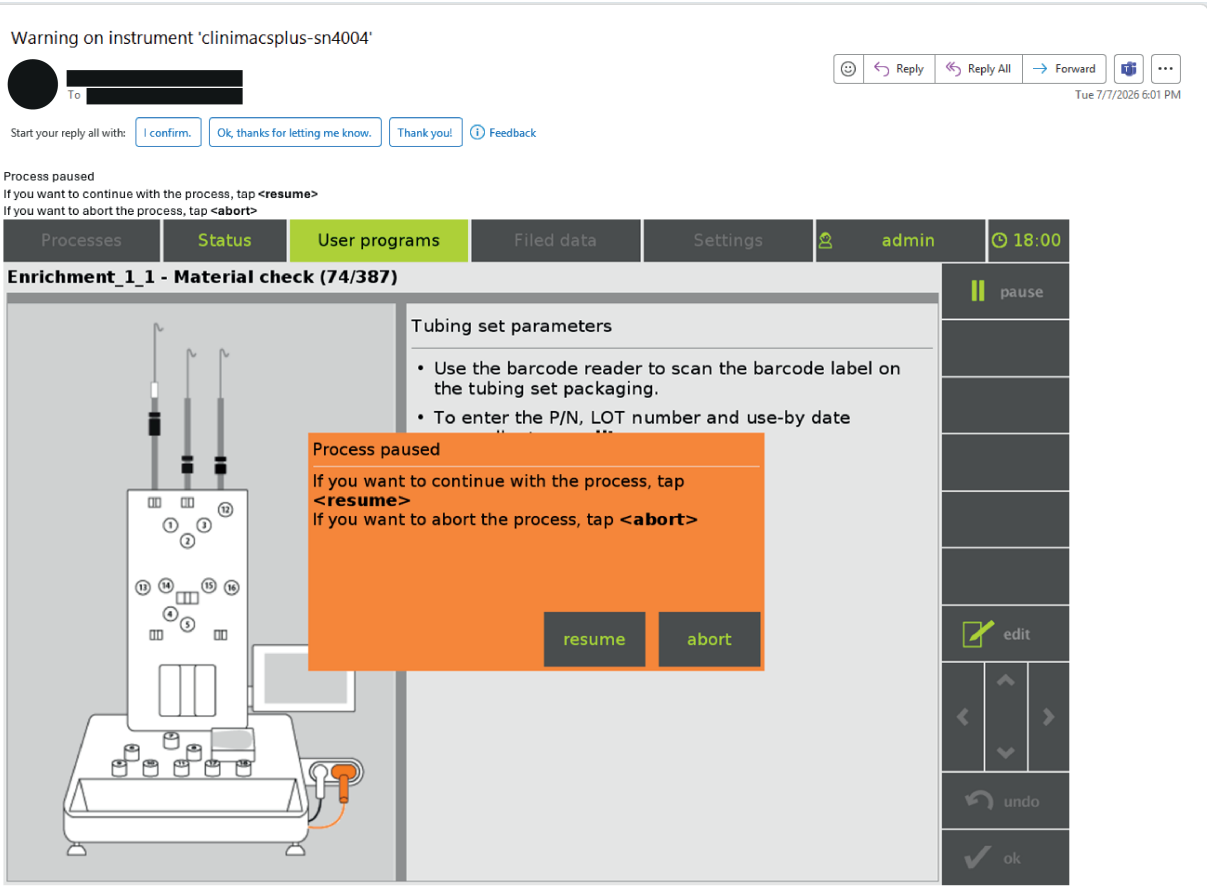


Figure 8.2: Example email in case of a warning

Prerequisites:

- An email server supporting SMTP or SMTPS. Make sure this server is reachable. Note down the IP address and the port of the server.
- A customer's email account, which can be used for authentication during setup.
- The instrument is connected to the Ethernet and network is enabled.

Setting up the instrument

1. To enter customer settings, go to **Settings** > **User settings** > **Customer Settings** and tap **run**.

2. To enter **Email Notification Settings**, tap **Email** in the toolbar.

3. To enter the value corresponding to the protocol used by the email server, go to **Email protocol** and tap **edit**. By default, SMTPS (1) is selected.

4. To enter the hostname or IP address of the email server, go to **Email server** and tap **edit**.

5. To enter the port used in the email server, go to **Server port** and tap **edit**.

   If the standard port is used, there is no need to edit this field.

Protocol	Default port	Alternative port
SMTP	25	2525, 465, 587
SMTPS	465	587 (using Transport Layer Security)

Table 8.1: Port for email server

6. If the email server requests authentication, proceed with step 7. Otherwise, proceed with step 9.
7. Go to **Requires authentication**, tap **edit** and set this field to 1.
8. Enter the authentication username and password for the email server under **Authentication: User** and **Authentication: Password**.

   IMPORTANT:
   Multiple instruments can share one authentication account. If required, consult your IT department for assistance.

9. To enter the email address of the sender, go to **Email: Sender** and tap **edit**. The **Email: Sender** can be the same as the authentication user.
10. To enter the email addresses of the recipients, go to **Email: Recipients** and tap **edit**. The recipients can also be a group email address.

    IMPORTANT:
    Multiple recipients may be entered, separated by a space.

11. If error messages should be received, go to **Notify on errors** and tap **edit**. Set to 1 to enable messages. By default, the **Notify on errors** function is disabled (value set to 0).
12. If warning messages should be received, go to **Notify on warnings** and tap **edit**. Set to 1 to enable messages. By default, the **Notify on warnings** function is disabled (value set to 0).
13. To enable email notifications, go to **Email notifications** and tap **edit**. Set to 1 to enable notifications. By default, email notifications are disabled (value set to 0).
14. After all required information is entered, the **Test** button in the toolbar is enabled. To send a test email, tap **Test** in the toolbar.

Adding further email certificates

1. To add a new email certificate, go to **Settings** > **User settings** > **Customer Settings** and tap **run**.
2. Tap **Email certificates** > **Add** and follow the instructions on the screen.

   IMPORTANT:
   The instrument provides some basic email certificates. If further certificates are required, these certificates must be uploaded.

8.5 Enabling network time synchronization

Network Time Protocol (NTP) is a network protocol that enables the synchronization of the time clock and centralized time management.

Only UMS users with the administrator role 'Administration tools user' or a user with the 'network setting tools user' role will be able to access the network settings. To enable NTP functionality on the instrument, follow these steps:

1. Go to **Settings** > **User Settings** > **Network Settings** and tap **run**.

2. To enable NTP and set time automatically, tap **NTP usage** and set value to 1, then tap **ok** in the input field.
3. To enter the hostname/IP address, tap **NTP: Primary server** or **NTP: Fallback server** and then **edit**. To confirm the input, tap **ok**.
4. Tap **save** and confirm that these changes are to be accepted and saved. The NTP server settings are enabled.
5. Reboot the system (see section 'Shutdown').

9

User management

This chapter provides comprehensive guidance on managing user accounts, roles, and access rights within the instrument software. It includes instructions on creating and modifying roles, adding and managing local and LDAP users, configuring password policies, and importing and exporting user management settings.

9.1 General information

The instrument's user management system (UMS) supports user authentication and role-based access control to support the 21 CFR Part 11 compliance.

- User authentication: username (also referred to as account ID) and password are required to login and use the instrument. Both local user management and LDAP authentication are supported.
- Role-based access control: user with different roles have different access rights. There are three terms defined in role-based access control: rights, roles and accounts.

9.1.1 Rights

Rights represent the minimum assignable unit of user actions and are defined by the software. Users cannot edit rights but only assign existing collections of rights to roles (see section 'Changing rights of roles'). For an overview of the different rights in the software, see section 'Roles and rights'.

9.1.2 Roles

Roles represent job functions or responsibilities within an organization. A collection of rights can be assigned to a role. The software provides default roles and supports customized roles. Important default roles are listed in Table 9.1.

Role	Rights
Administration tools user	to access tools for administrating the instrument (suggested for administrators)
Application x.y Operator	to run a specific application with version number x.y
ATS User	to access Audit Trail including viewing, exporting and deleting it
Common tools user	to access common tools, for example info, license, shutdown, and user settings (suggested for all users)
File management user	to access Backup Filed Data tool and Custom Files tool
Injected programs	to run injected programs
Network Utilities	to access network utilities
Operator	to operate the instrument
Set time User	to set the time of the instrument
Support tools user	to access tools that support the execution of applications
UM Administrator	to access the user management system allowing to manage accounts
UM User	to start user applications

Table 9.1: Overview of default roles

9.1.3 Accounts

Accounts represent individual users. There should be a one-to-one relation between an individual and an account ID in a Good Manufacturing Practice (GMP) environment. Upon installation, an administrator account with all roles is created. This account allows the user to create new roles and new accounts as needed.

A conventional UMS setup could be:

- An administrator manages accounts and the instrument. The administrator role would typically allow the setup and change of accounts and provides access to file management and advanced tools for instrument settings.
- A user starts and runs applications on the instrument. Based on the customer's user management, the user account would allow to run a particular set of applications, support tools, and troubleshooting tools. There can be more than one customer-defined user type, and each user may be assigned one or more roles.

IMPORTANT:

- For a user, the role 'UM User' must be assigned. For an administrator, the role 'UM Administrator' must be assigned.
- It is highly recommended to establish a so-called 'break-glass solution' for emergency situations. This could be an additional administrator account for emergency usage. The credentials of the break-glass account should be stored in a safe place and may only be available to certain people.
- The authentication procedure should be described and implemented within the quality management system of the facility. All users and administrators need to be trained accordingly.
- If the LDAP connection fails, use a local user account to access the instrument.

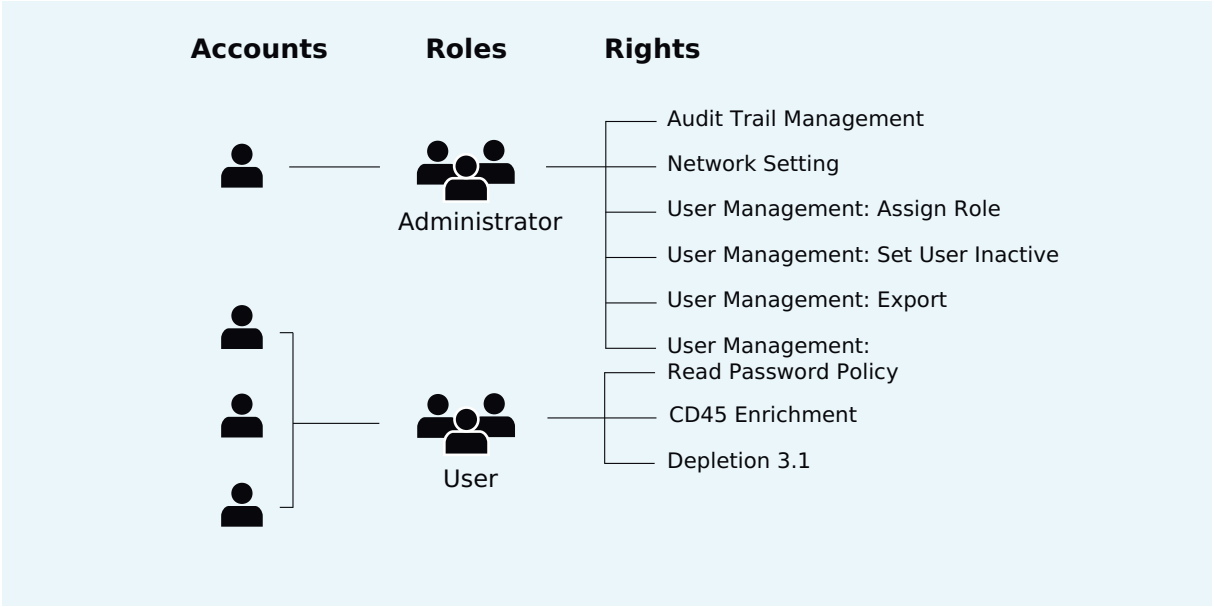


Figure 9.1: Exemplary accounts, roles, and rights

9.2 Managing roles and accounts

9.2.1 Accessing the user management system

IMPORTANT:
A user must have the role 'UM Administrator' to configure the UMS.

To enter the UMS (see Figure 9.2), navigate to **quick access menu** > **User setup**.

The UMS has four tabs: **Users**, **LDAP Groups**, **Roles**, and **Configuration**. By default, the **Users** tab is selected.

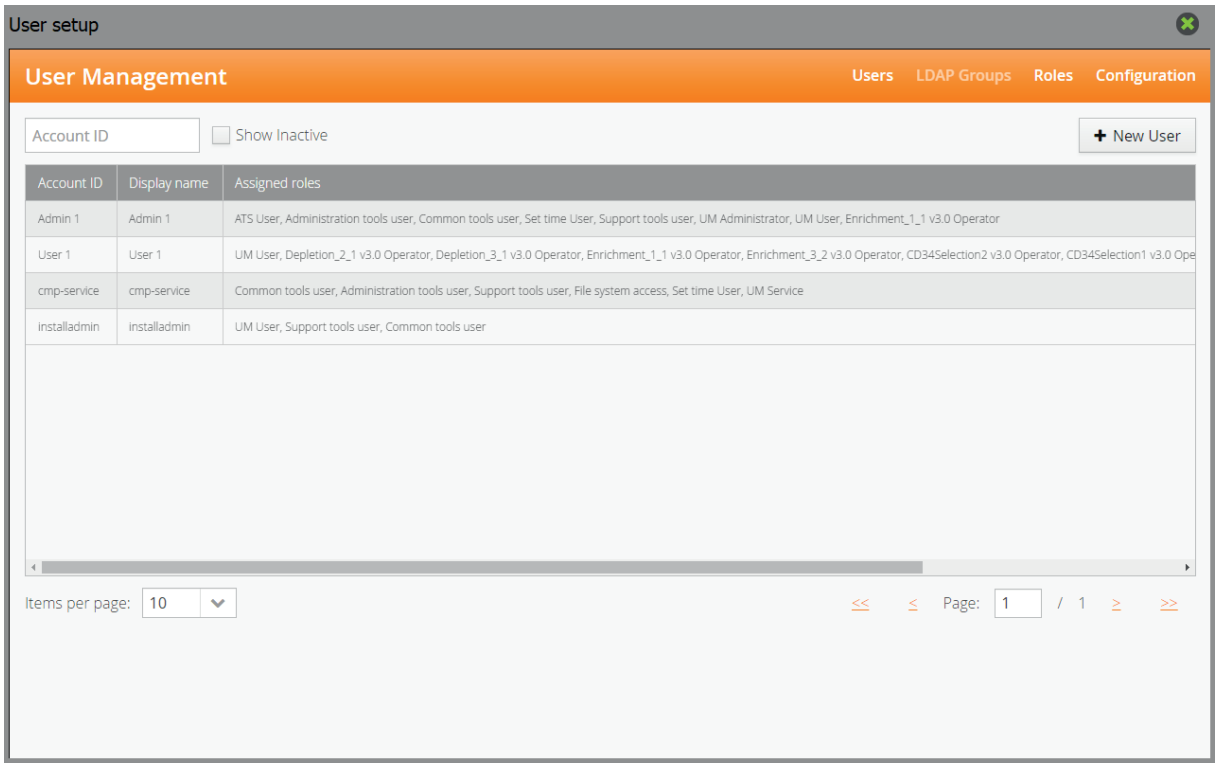
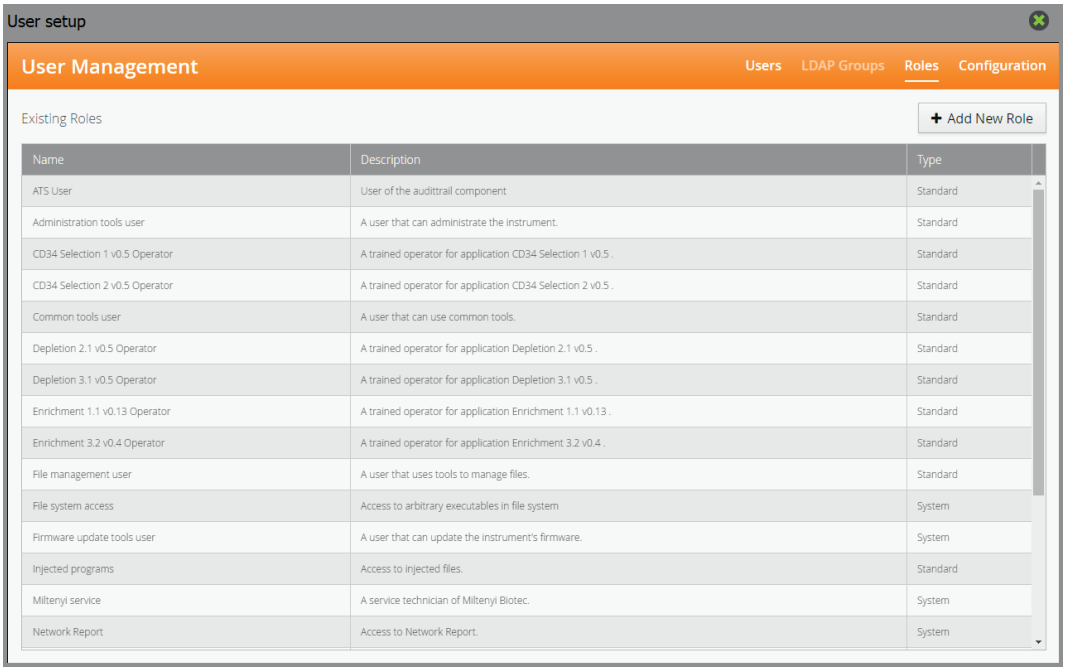


Figure 9.2: User management menu

9.2.2 Creating a new role

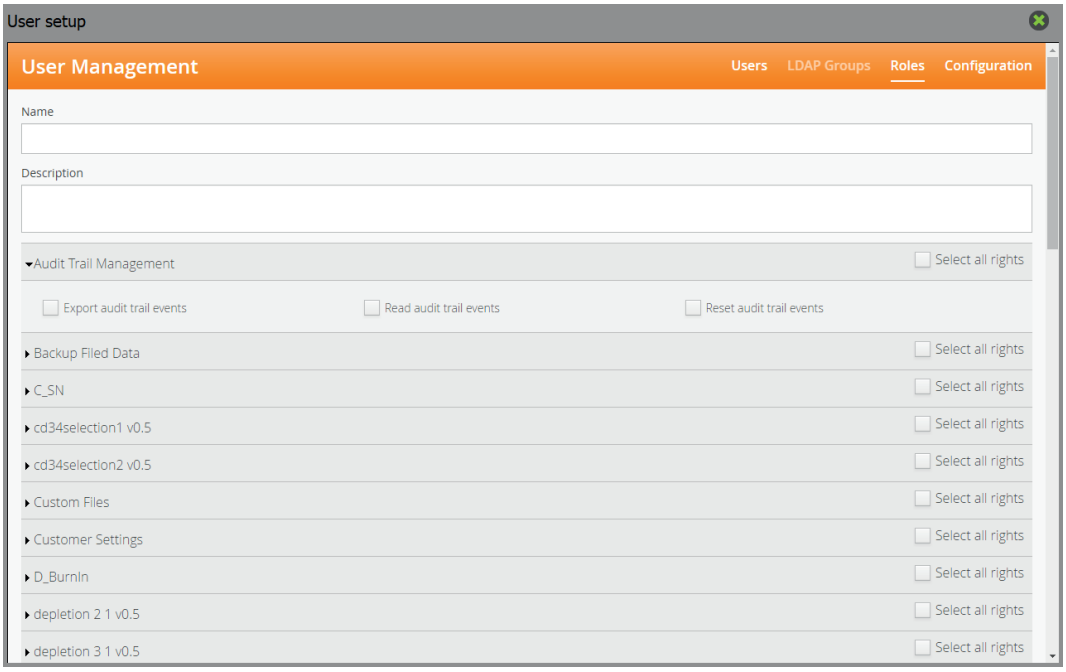
1. Tap **Roles** in the **User Management**.

   A list of existing roles is shown:



2. Tap + Add New Role.

   A new role definition page is shown:



3. Enter the name and description of the new role and select the required rights.

4. Tap save at the bottom of page. The new added role is shown in the list of existing roles and can be assigned to a user.

9.2.3 Changing rights of roles

1. Find and select the role in the list of existing roles (User management > Roles).
2. Select or deselect the desired rights.
3. Scroll down to the bottom and tap save.

9.2.4 Adding local users

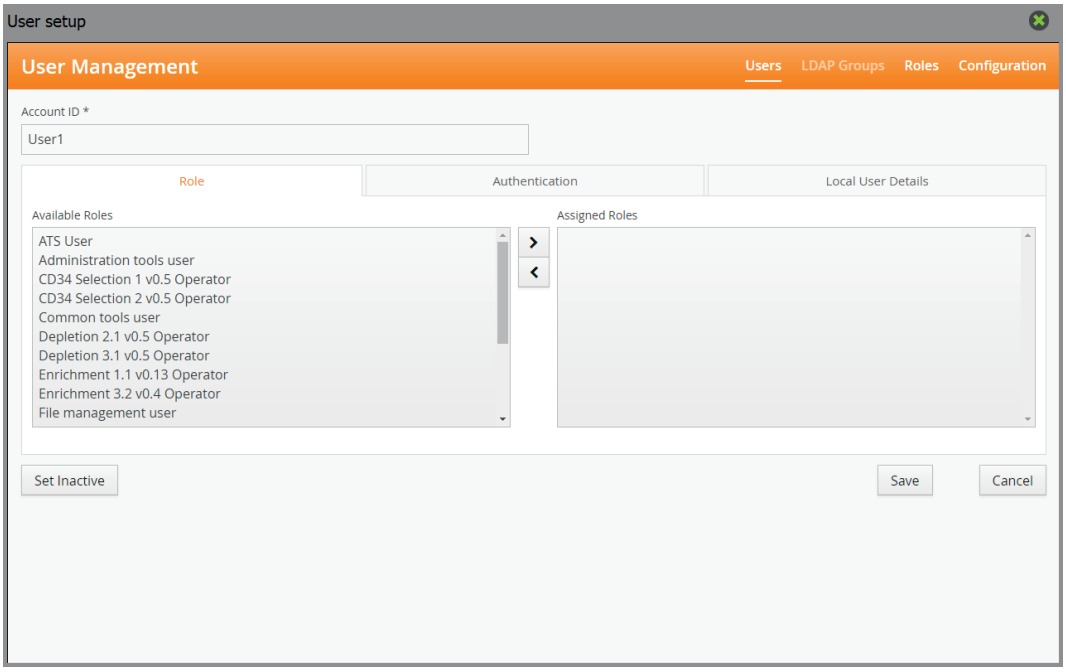
1. Select the Users tab in the user management system and tap + New User.

IMPORTANT:
A user must have the role 'UM Administrator' to create a new account.

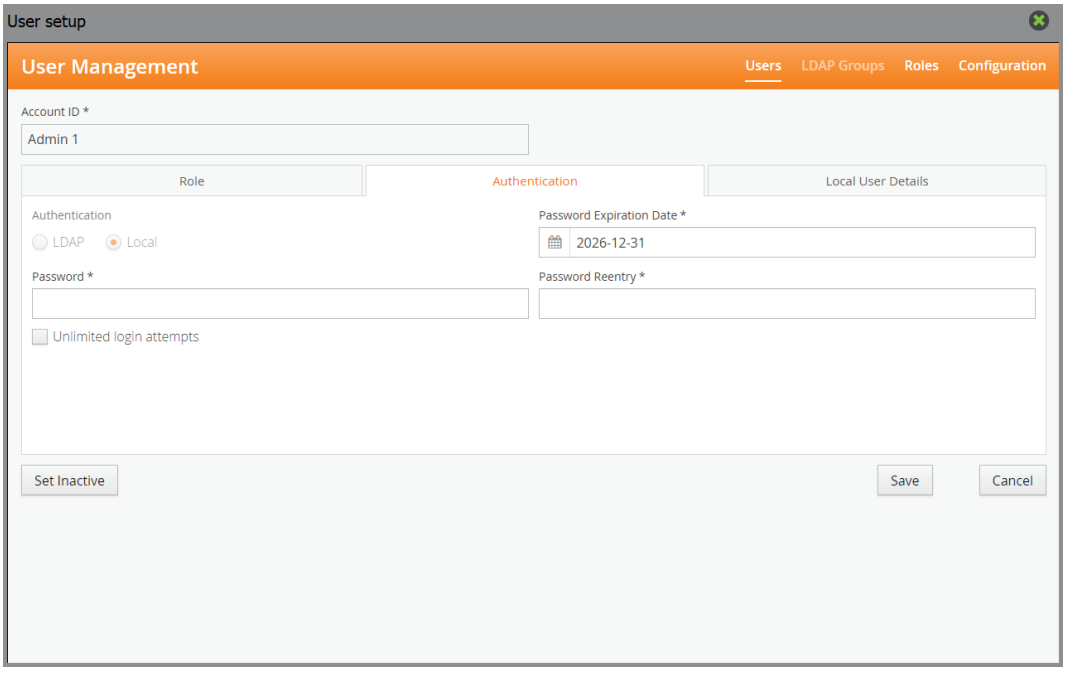
2. Enter an account ID.

   This account ID must be unique and has a one-to-one relationship with end users. The account ID corresponds to the username when logging in. If Active Directory (AD) is configured, the software checks if this ID is registered in the AD server. If the ID is not found, a local account is created. If the ID is found, the AD account is used by default. To change an LDAP account to a local account, follow step 4.

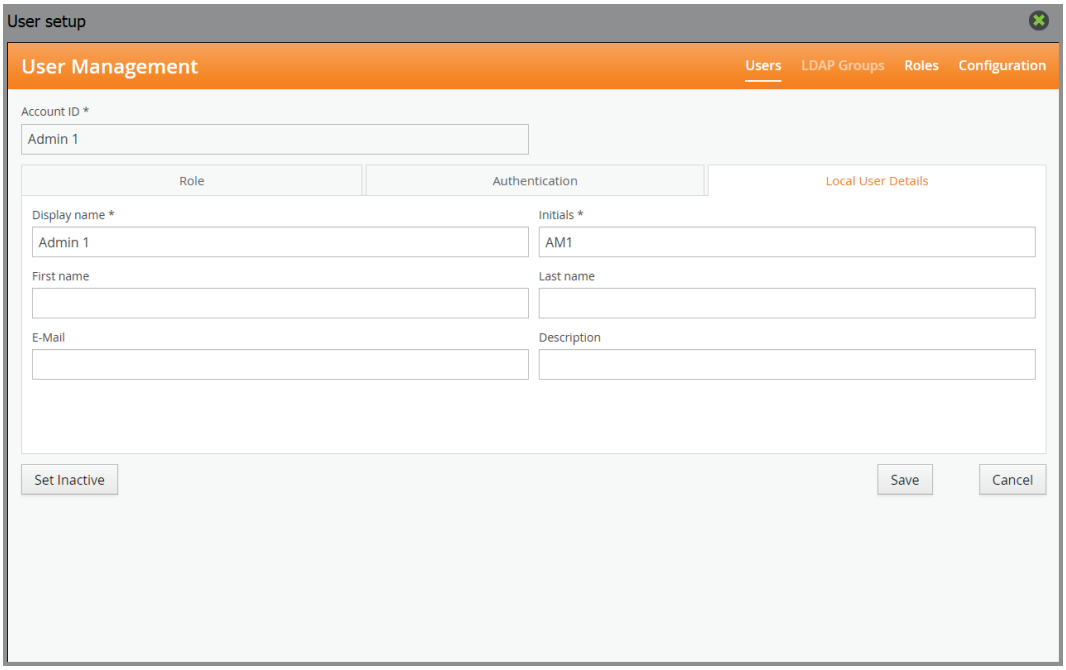
3. To assign the corresponding roles to this account, select the entry in **Available Roles** in the **Role** tab, and tap [›]. To remove an assigned role of this account, select the entry in **Assigned Roles** and tap [‹].



4. If LDAP is configured and the Account ID is found on the AD server, the user can choose between authentication via the AD server or the local database (see **Authentication** tab). For a local user, enter the password and set the expiration date, following the password policy (see section 'Configuring password policy').



5. In the **Local User Details** tab, set more detailed information of this account.

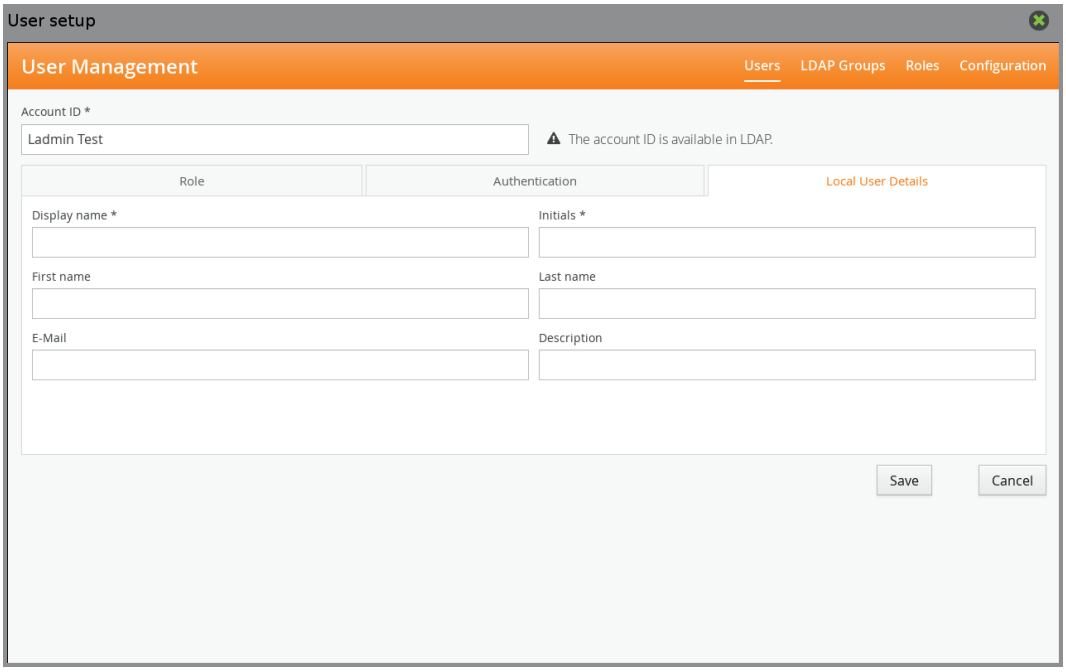


6. Tap **save**. The new added account is shown in the account list.

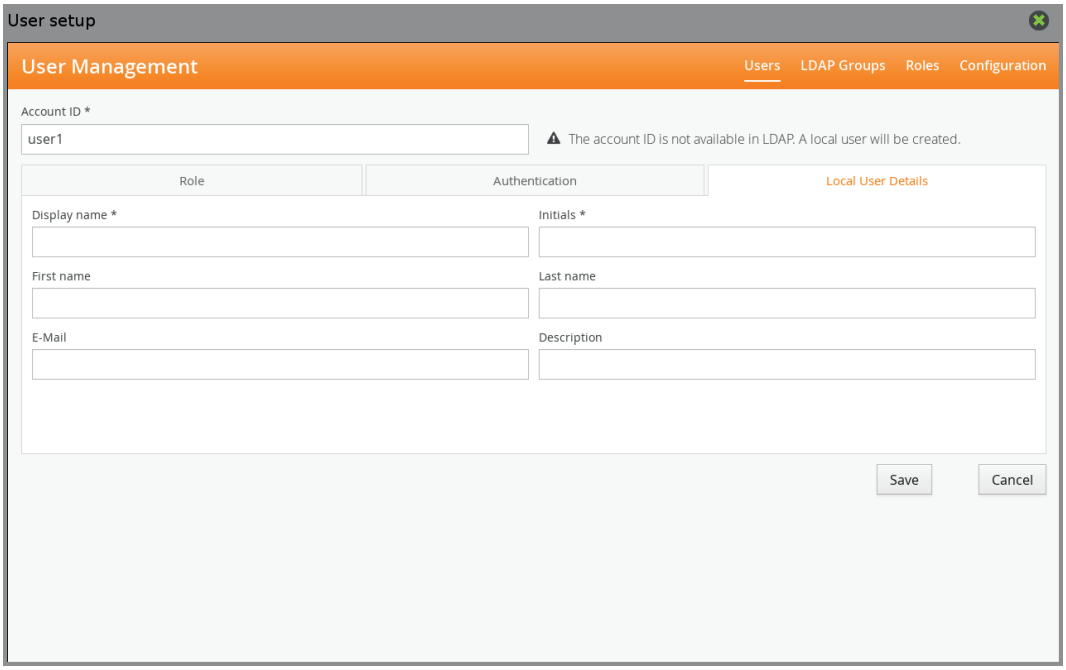
9.2.5 Adding LDAP users

1. Select the **Users** tab in the user management system and tap **+ New User**.

2. Enter the LDAP account ID. The software checks if this ID is registered in the AD server. If the user already exists, more information is filled using the attribute mapping.



If the user is not registered in the AD, a new local user is created.



3. To assign roles, tap **Role** and select the desired roles.

4. Tap **save**. The user can use the LDAP account ID and the corresponding password to login.

9.2.6 Adding LDAP groups

IMPORTANT:
Ensure to add the correct 'UM Administrator' or 'UM User' to ensure a proper login.

1. Select **LDAP Groups** in the menu bar and tap **+ Assign Roles to New Group**.

2. Enter the group name. The system automatically checks if this group exists in LDAP.
3. To assign roles to this group, select the roles in Available Roles and tap ›. To remove an assigned role of this group, select the entry in Assigned Roles and tap ‹.
4. Tap save.

9.2.7 Changing assigned roles of users or LDAP groups

1. Select a user in the Users tab or, for an LDAP group, select the desired group in the LDAP Groups tab.
2. To assign additional roles to the user or LDAP group, select the entry in Available Roles in the Role tab and tap ›. To remove assigned roles of this account, select the entry in Assigned roles and tap ‹.
3. Tap Save at the bottom of the Role tab.

9.2.8 Deactivating local users

IMPORTANT:
A local user cannot be deleted, it can only be deactivated.

1. Select a local user from the Users tab.

2. Tap Set Inactive at the bottom of the user configuration page.
   A pop-up window appears stating the successful deactivation of the user.

3. To return to the user list, tap Save at the bottom of the screen. The inactive account is not shown in the user list. Nevertheless, the account is still stored on the instrument. To set this account active again, check Show Inactive and follow the same procedure as described in section 'Changing assigned roles of users or LDAP groups'.

9.2.9 Deleting LDAP users

1. Select an LDAP user or LDAP group from the user list.
2. In the user configuration page, tap Delete.
3. To confirm and return to the user list, tap Save.

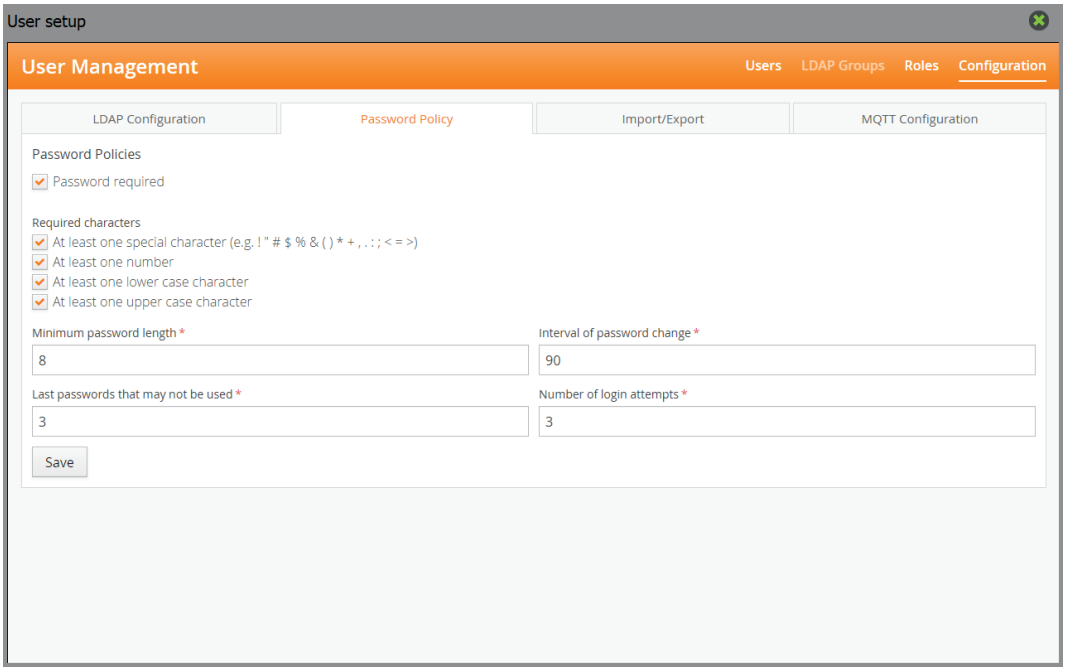
9.3 Configuring password policy

IMPORTANT:

- Changing the password policy only affects the users created afterwards. The already created users are not affected.
- The password policy is overruled by the LDAP password policy for the LDAP account.

1. To configure password policy, tap Configuration on the top right corner.

2. Select the **Password Policy** tab.



The following can be configured:

- Required characters
- Password length
- Password expiration time (in days)
- Last password that may not be used
- Maximum number of login attempts

9.4 Importing and exporting user management settings

IMPORTANT:
Only UMS users with the administrator role 'Administration tools user' are able to access this application.

The UMS configuration can be transferred from one instrument to another. The process involves two stages (see Figure 9.3):

1. Copy between USB flash drive and UMS exchange folder using UMS Exchange Tool.
2. Import/Export into UMS in the User Management Configuration.

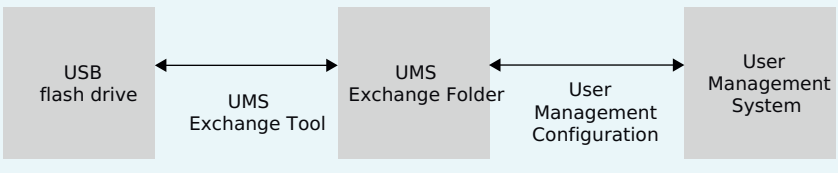


Figure 9.3: Transfer of UMS settings

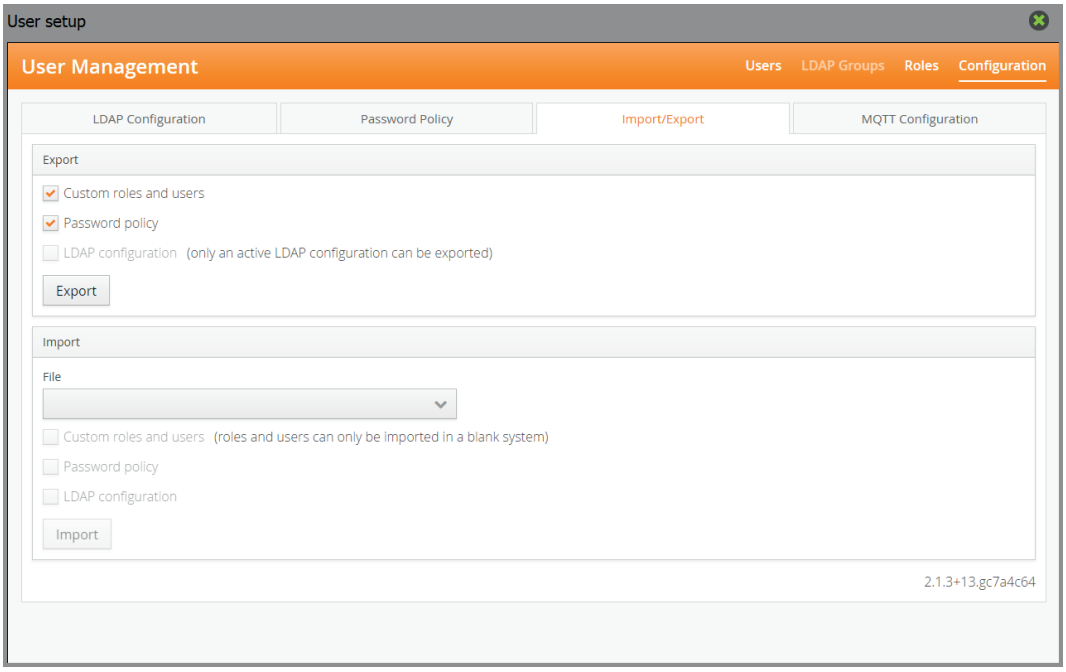
This procedure applies for both of the following files:

- Import Secure Sockets Layer (SSL) certificate files to set up a secure LDAP connection.
- Import and export UMS setting files for backup or reuse on other UMS instances.

9.4.1 Exporting user management settings

1. Insert a USB flash drive.

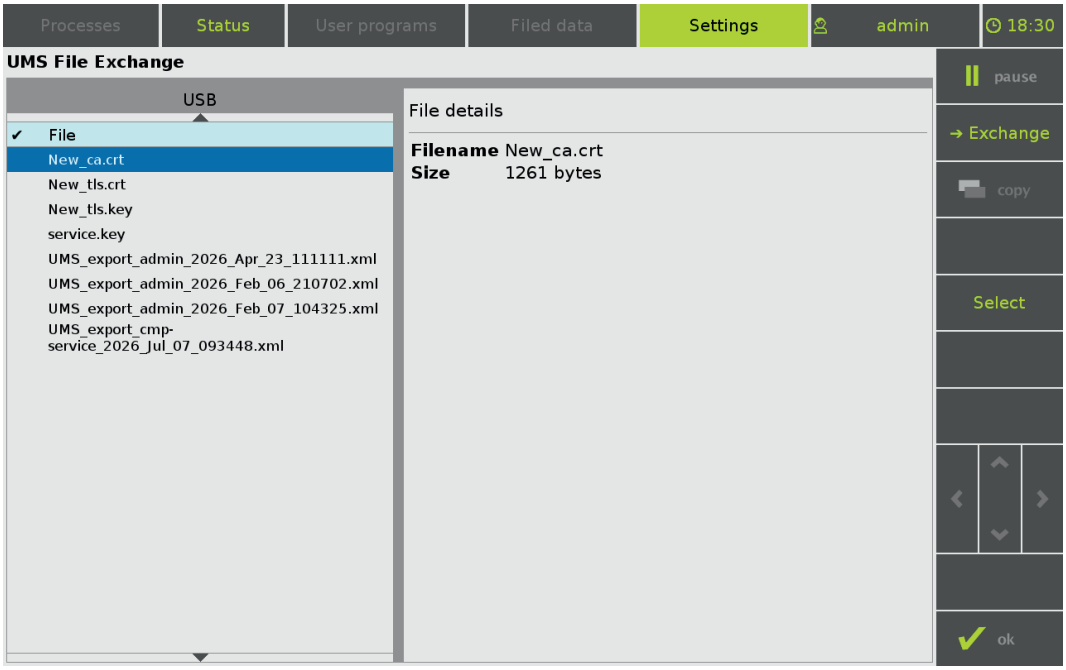
2. Go to **User Management** > **Configuration** > **Import/Export**.



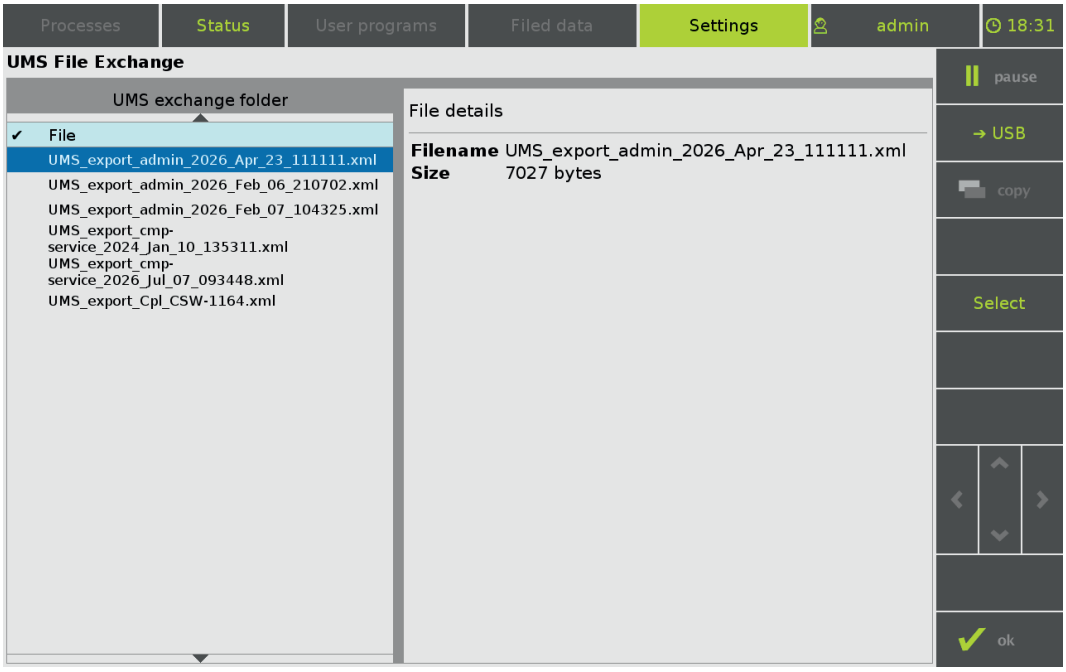
3. Tap **Export**. The UMS settings are exported to UMS Exchange Folder on the instrument.

4. To enter the **UMS File Exchange**, go to **Settings** > **Tools** > **UMS File Exchange**, and tap **run**.

5. If USB is shown on the left column, tap Exchange to list the contents of the UMS exchange folder.



The files in the UMS exchange folder will be shown in the left column:



6. Select the files to be transferred to the UMS and tap Select.

7. Once all the files to be transferred are selected, tap copy to start the transfer.

9.4.2 Importing user management settings

IMPORTANT:
Roles and users can only be imported into a blank system. Once the UMS has been modified, it is no longer possible to import user management settings.

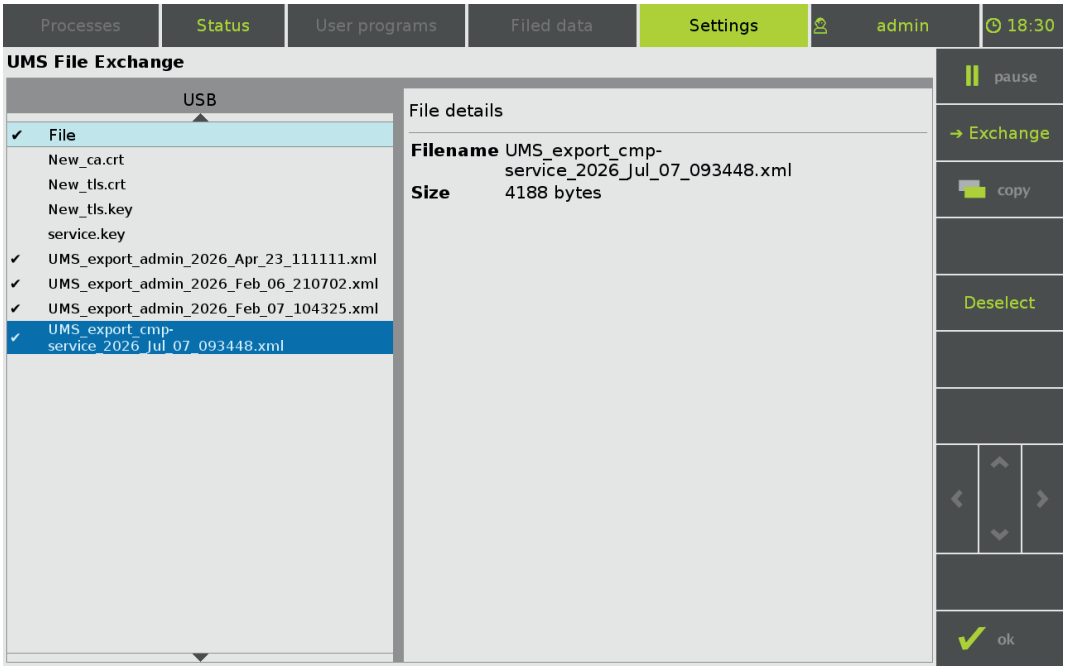
1. Insert a USB flash drive. Ensure that the files are in the root folder of the USB flash drive (files in subfolders will not be recognized).

2. Go to **Process** > **Tools** > **UMS File Exchange** and tap **run** to enter the **UMS File Exchange** tool. A list of files is shown on the left side.

3. When the UMS exchange folder is shown, tap **USB** in the toolbar. Make sure **USB** is shown on top of the file list in the left column.

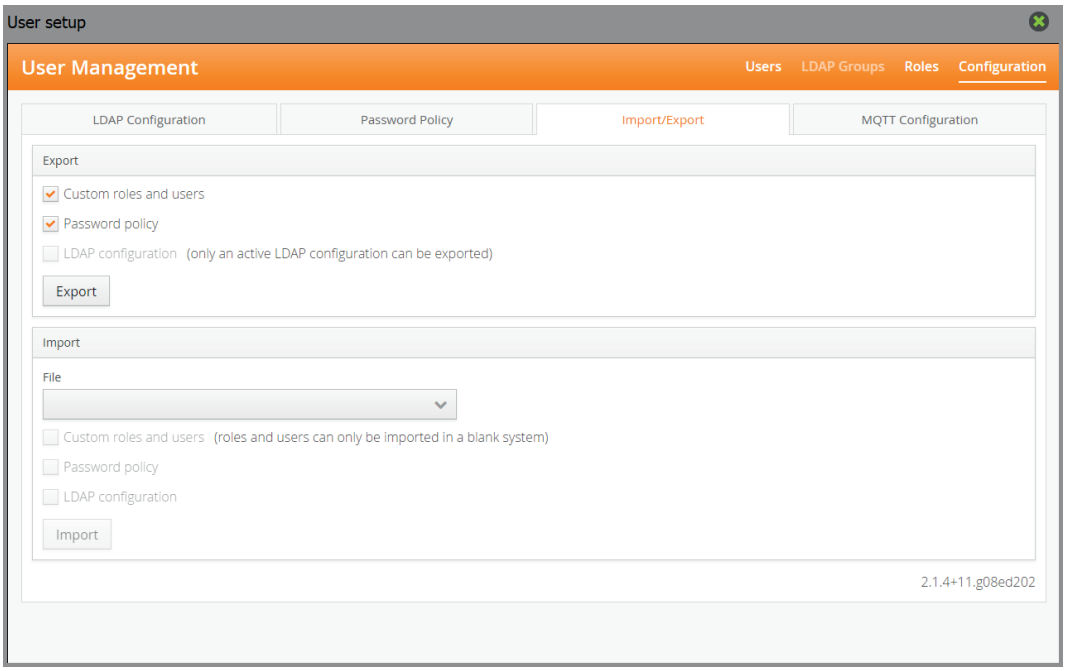


4. Select the files to be transferred and tap **Select**. To deselect the file, choose a selected file and tap **Deselect**.



5. Once all the files to be transferred are selected, tap **copy** to start the transfer.

6. Go to > **User setup** > **Configuration** > **Import/Export**.



7. Select the file in **Import** and tap **Import**.

10

Troubleshooting

This chapter gives troubleshooting information and how to act in the case of an error.

10.1 Service information

Record below the serial number located on the rear of the CliniMACS Plus Instrument. Refer to these numbers when calling Miltenyi Biotec Technical Support to obtain information or request service on the instrument.

Catalog no. (REF): _____

Serial no. (SN): _____

Software version: _____

IMPORTANT:
The software version is shown during the start-up phase of the instrument.

10.2 Miltenyi Biotec Technical Support

In any case of instrument malfunction or a process failure that cannot be corrected by the user, contact the Miltenyi Biotec Technical Support team:

+49 2204 8306-3803

technicalsupport@miltenyi.com

Visit www.miltenyibiotec.com for local Miltenyi Biotec Technical Support contact information.

10.3 Error messages

The instrument and software can have malfunctions. Error messages are shown on the screen and marked as such. If the error cannot be corrected by the user, record the shown error number and contact Miltenyi Biotec Technical Support as soon as possible. One possible error message is shown in Figure 10.1.

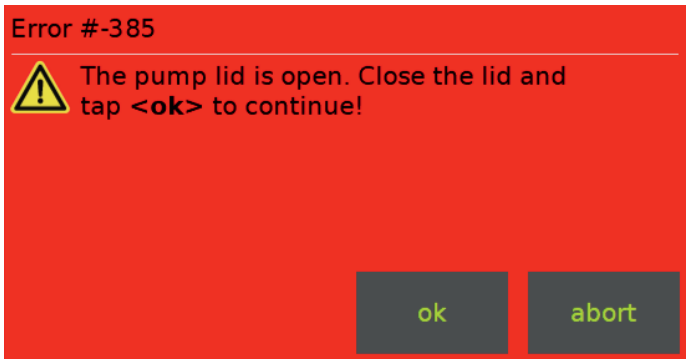


Figure 10.1: Error message

For details regarding application-specific warning and error messages, refer to the 'Troubleshooting' chapter of the CliniMACS Plus Applications user manual.

10.3.1 Login issues

Pop-up window not related to wrong user credentials or missing access rights

If a pop-up window appears while trying to log in, which is not related to incorrect user credentials or insufficient access rights, proceed as follows:

Retry login

1. Confirm the pop-up window by tapping ok.
2. Wait for about 30 seconds.
3. Enter the user credentials again. If login still fails, contact a system administrator.

Contact a system administrator

Contact a system administrator to verify the correctness of username and password and the access rights of the account. For more information, see chapter 'User management'. If login still fails, contact Miltenyi Biotec Technical Support.

11

Legal notes

11.1 Limited warranty

Except as stated in a specific warranty statement, which may accompany this Miltenyi Biotec product, or unless otherwise agreed in writing by a duly authorized Miltenyi Biotec representative, Miltenyi Biotec's warranty for products purchased directly from Miltenyi Biotec shall be subject to the terms and conditions of sale under which it was provided to you by the respective Miltenyi Biotec sales organization. These terms and conditions are available on request or at www.miltenyibiotec.com. The applicable terms and conditions of sale may vary by country and region. Nothing herein should be construed as constituting an additional warranty.

For products purchased from third-party retailers or resellers (e.g., purchased from an Authorized Distributor of Miltenyi Biotec), different terms and conditions may apply.

To determine the warranty that came with your product, see your packing slip, invoice, receipt or other sales documentation. Some components of a product combination you purchased may have a shorter warranty than that listed on your packing slip, invoice, receipt or other sales documentation (e.g., goods subject to shelf life and obsolescence).

Miltenyi Biotec's warranty for this product only covers product issues caused by defects in material or workmanship during normal use. It does not cover product issues caused by any other reason, including but not limited to product issues due to use of the product in a manner other than specifically described in this manual, for example: inappropriate or improper use; incorrect assembly or installation by an operator or a third-party; reasonable wear and tear; negligent or incorrect operation, handling, storage, servicing, or maintenance; non-adherence to the operating instructions; unauthorized modification of or to any part of this product; or use of inappropriate consumables, accessories, or work materials.

Miltenyi Biotec's warranty does not cover products sold AS IS or WITH ALL FAULTS or consumables. Nothing herein should be construed as constituting an additional warranty.

Miltenyi Biotec must be informed immediately if a claim is made under such warranty. If a material or manufacturing defect occurs within the warranty period Miltenyi Biotec will take the appropriate steps to restore the full usability of the instrument.

Limitation on damages

Miltenyi Biotec shall not be liable for any incidental or consequential damages for breach of any express or implied warranty or condition on this product.

Some countries/states or jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitations or exclusions may not apply to you. This warranty statement gives you specific legal rights and you may have other rights, which vary from state to state or jurisdiction to jurisdiction.

11.2 Trademarks

CliniMACS, MACS, and the Miltenyi Biotec logo are registered trademarks or trademarks of Miltenyi Biotec B.V. & Co. KG and/or its affiliates in various countries worldwide. All other trademarks mentioned in this document are the property of their respective owners and are used for identification purposes only.

12

Appendix

12.1 Glossary

An overview of symbols and general terms used for the CliniMACS Plus System is provided in the CliniMACS Plus Instrument user manual.

12.1.1 Abbreviations

AD	Active Directory
ATS	Audit trail system
CAN	Controller Area Network
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
GMP	Good Manufacturing Practice
GUI	Graphical user interface
ICMP	Internet Control Message Protocol
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LDAPS	Secured version of Lightweight Directory Access Protocol
NTP	Network Time Protocol
REF	Catalog number
SMB	Server Message Block
SMTP	Simple Mail Transfer Protocol
SMTPS	Secured version of Simple Mail Transfer Protocol
SN	Serial number
SSL	Secure Sockets Layer
UDP	User Datagram Protocol
UMS	User management system
UTC	Coordinated Universal Time

12.1.2 Terms

The following terms are software-specific. The general CliniMACS Plus-related terms are listed in the CliniMACS Plus Instrument user manual.

Active Directory	A service that stores and manages information about users, computers, and other resources in a network, allowing administrators to control access and security from one central place
Application process	Software for cell processing developed by Miltenyi Biotec

Audit trail system	A software component that tracks and records the events, actions, user inputs, and changes made within the CliniMACS Plus Software
Domain Name System	System that translates human-readable domain names (such as example.com) into IP addresses so devices can communicate with each other over a network
Dynamic Host Configuration Protocol	Network protocol that automatically assigns IP addresses and other network settings (such as the default gateway and DNS servers) to devices on a network
Internet Control Message Protocol	Network protocol that sends error and status messages between network devices to help diagnose connectivity and communication problems
Lightweight Directory Access Protocol	Application protocol for accessing and maintaining distributed directory information services over an Internet Protocol network
MD5	Algorithm used to create checksum to verify data integrity against unintentional corruption
Network Time Protocol	Network protocol that synchronizes the clocks of devices on a network to ensure they all use the same date and time
Secure Sockets Layer	Network protocol that encrypts data exchanged between devices to help keep information private and secure during transmission
Server Message Block	Communication protocol used to share files, printers, serial ports, and miscellaneous communications between nodes on a network
Simple Mail Transfer Protocol	Communication protocol for electronic mail transmission
Standard application process	A pre-validated application process provided by Miltenyi Biotec
User Datagram Protocol	Network protocol that transfers data quickly between devices without establishing a connection, making it useful for real-time applications
User management system	A software component to manage and control user access to the various functions on the instrument

12.2 Roles and rights

Each process, tool, and setting is associated with specific rights, for example a 'Show' right and a 'Start' right. With the 'Show' right, the process, tool, or setting becomes visible in the **Processes** or **Settings** tab for the respective role. To be able to run the process, tool, or setting, the 'Start' right needs to be assigned to the role. More complicated components like audit trail and user management have more detailed rights.

Software component	Rights
Application processes	• Show process • Start process
Audit Trail Management	• Export audit trail events • Read audit trail events • Reset audit trail events
Instrument	• Show injected programs • Start injected programs
Tools • Backup Filed Data • Custom Files • Info • Instrument check • License • Sealer • Shutdown • UMS File Exchange	• Show tool • Start tool
User Management	• Assign role • Configure LDAP connection • Create role • Create user • Export • Import • Overwrite user/role details • Read Password Policy • Read details of foreign account • Read details of own account • Read own user details • Read rights of foreign account • Read rights of own account • Read role • Read user details • Set user active • Set user inactive • Unlock user • Update Password Policy • Update own user details • Update role • Update user details

Software component	Rights
User settings • Customer Settings • Network Settings • Network Utilities • Set Time • Settings Exchange • SetVolume • UMS Settings	• Show setting • Start setting

Table 12.1: Overview of rights defined in the software

Roles	Tools/rights
Administration tools user	User that can administrate the instrument (suggested for administrators) • Customer settings • Info • Network settings • Set time • Settings Exchange • Set Volume • UMS File Exchange • UMS Settings
Application x.y Operator	Trained user for application x.y
ATS User	User of the audit trail component • Audit Trail Management
Common tools user	User that can use common tools (suggested for all users) • Info • License • Shutdown
File management user	User that uses tools to manage files • Backup Filed Data • Custom Files
Injected programs	User that can show and start injected programs
Network Utilities	User that can show and start network utilities
Operator	User that can operate the instrument • Shutdown
Set time User	User that can change the time of the instrument • Set Time
Support tools user	User that can use tools that support the execution of applications • Instrument Check • Sealer
UM Administrator	Administrator of the user management component • User Management
UM User	Custom User • User Management: Read details of own account • User Management: Read rights of own account

Table 12.2: Default roles

Miltenyi Biotec

Germany/Austria
Miltenyi Biotec B.V. & Co. KG
Friedrich-Ebert-Straße 68
51429 Bergisch Gladbach
Germany
+49 2204 8306-0
+49 2204 85197
macsde@miltenyi.com

USA/Canada
Miltenyi Biotec, Inc.
1201 Clopper Road
Gaithersburg, MD 20878
USA
800 FOR MACS
+1 866 811 4466
+1 877 591 1060
macsus@miltenyi.com

Australia
Miltenyi Biotec Australia Pty. Ltd.
Unit 11, 2 Eden Park Drive
Macquarie Park NSW 2113
Australia
+61 2 8877 7400
+61 2 9889 5044
macsau@miltenyi.com

Benelux
Miltenyi Biotec B.V.
Dellaertweg 9C
2316 WZ Leiden
The Netherlands
macsnl@miltenyi.com
Customer service for:
The Netherlands
0800 4020120
0800 4020100
Belgium
0800 94016
0800 99626
Luxembourg
800 24971
800 24984

China
Miltenyi Biotec Technology & Trading (Shanghai) Co., Ltd.
Room A401, 4/F
No. 1077, Zhangheng Road
Pudong New Area
201203 Shanghai
P.R. China
+86 21 6084 0210
+86 21 6235 0953
macscn@miltenyi.com.cn

France
Miltenyi Biotec SAS
10 rue Mercoeur
75011 Paris
France
+33 1 56 98 16 16
macsfr@miltenyi.com

Hong Kong
Miltenyi Biotec Hong Kong Ltd.
Unit 301, Lakeside 1
No. 8 Science Park West Avenue
Hong Kong Science Park
Pak Shek Kok, New Territories
Hong Kong
+852 3751 6698
+852 3619 5772
macshk@miltenyi.com.hk

India
Miltenyi Biotec India Pvt. Ltd.
Vatika Business Centre,
Floor No. 6
Divya Sree Omega
Kondapur, Serilingampally
K.V. Rangareddy
Telangana 500084
India
+91 040 45175910
macsin@miltenyi.com

Italy
Miltenyi Biotec S.r.l.
Via Paolo Nanni Costa, 30
40133 Bologna
Italy
+39 051 6460 411
+39 051 6460 499
macsit@miltenyi.com

Japan
Miltenyi Biotec K.K.
NEX-Eitai Building 5F
16-10 Fuyuki, Koto-ku
Tokyo 135-0041
Japan
+81 3 5646 8910
+81 3 5646 8911
macsjp@miltenyi.com

Nordics and Baltics
Miltenyi Biotec Norden AB
Medicon Village
Scheeletorget 1
223 81 Lund
Sweden
macsse@miltenyi.com
Customer service for:
Sweden
0200 111 800
+46 280 72 99
Denmark
80 20 30 10
+46 46 280 72 99
Norway, Finland, Iceland, and Baltic countries
+46 46 280 72 80
+46 46 280 72 99

Singapore
Miltenyi Biotec Asia Pacific Pte Ltd.
438B Alexandra Road, Block B
Alexandra Technopark
#06-01
Singapore 119968
+65 6238 8183
+65 6238 0302
macssg@miltenyi.com

South Korea
Miltenyi Biotec Korea Co., Ltd.
Donggeuk 7F
562 Nonhyeon-ro
Gangnam-gu
Seoul 06136
South Korea
+82 2 555 1988
+82 2 555 8890
macskr@miltenyi.com

Spain
Miltenyi Biotec S.L.
C/Virgilio 2, Edificio II, Planta –1
28223 Pozuelo de Alarcón, Madrid
Spain
+34 91 512 12 90
+34 91 512 12 91
macses@miltenyi.com

Switzerland
Miltenyi Biotec Swiss AG
Soodstrasse 52
8134 Adliswil
Switzerland
+41 32 623 08 47
+49 2204 85197
macsch@miltenyi.com

United Kingdom
Miltenyi Biotec Ltd.
Almac House, Church Lane
Bisley, Surrey GU24 9DR
United Kingdom
+44 1483 799 800
+44 1483 799 811
macsuk@miltenyi.com

www.miltenyibiotec.com

210-005-795/01 | Issued: 2026-09

Miltenyi Biotec provides products and services worldwide. Visit **www.miltenyibiotec.com/local** to find the nearest Miltenyi Biotec contact.