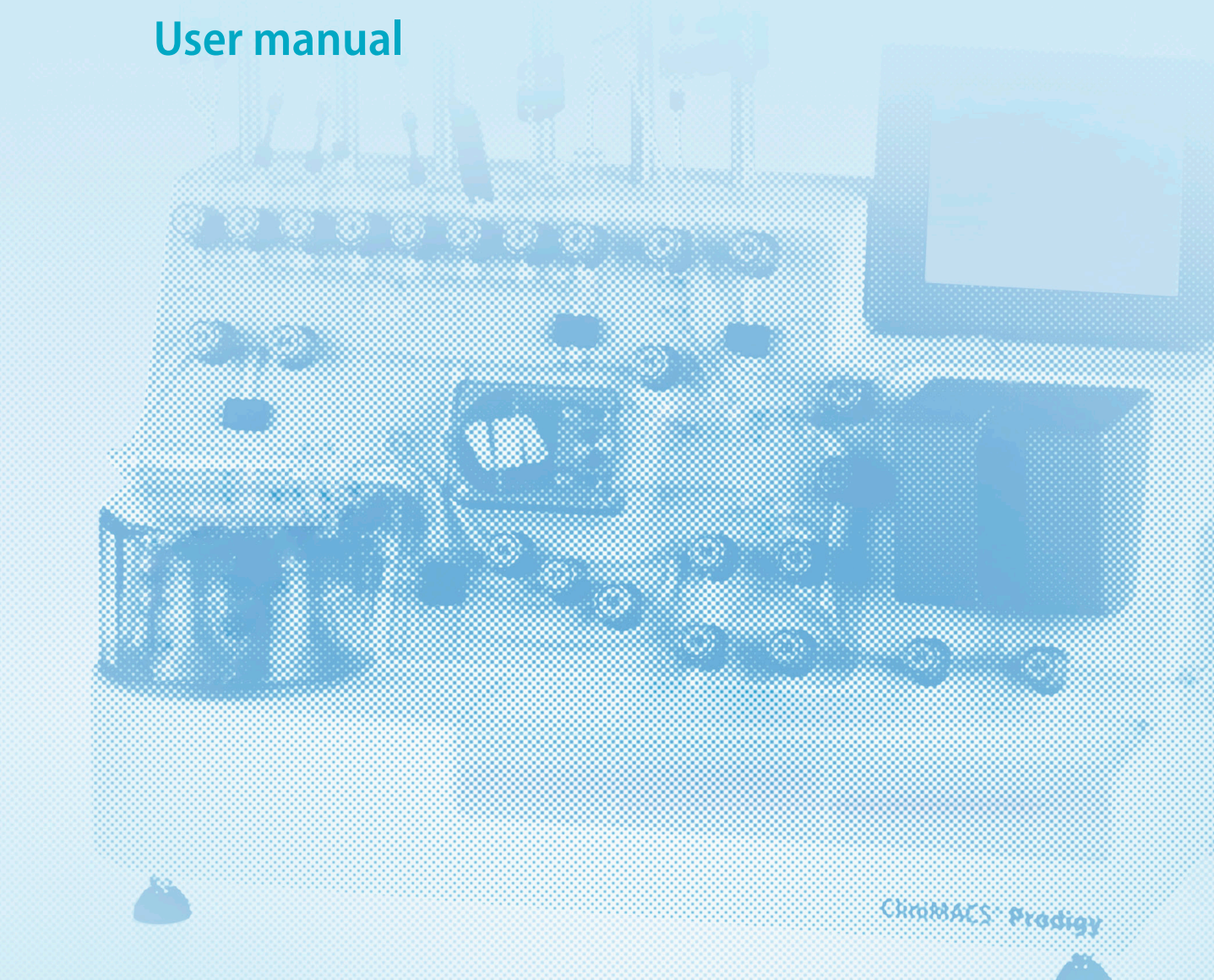
Miltenyi Biotec

CliniMACS Prodigy® 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 Prodigy System are included in the Australian Register of Therapeutic Goods (ARTG) and are therefore approved for supply: CliniMACS Prodigy, CliniMACS CD34 Reagent, CliniMACS Prodigy Tubing Sets, and CliniMACS PBS/EDTA Buffer. Only those products which are included in the ARTG may be used in Australia. CliniMACS MicroBeads are for research use only and not for human therapeutic or diagnostic use.

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

CliniMACS Prodigy® Software

User manual

Software version 2.2

Issued: 2026-01

210-004-964/02

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

Essential information

This user manual provides instructions, warnings, precautions, notifications, and other important information for the use of the CliniMACS Prodigy Software. For details on instrument related information such as touchscreen and general setup, refer to the CliniMACS Prodigy Instrument user manual.

⚠ WARNING

The operation of the CliniMACS Prodigy System must be performed by trained operators only. Before putting the system into operation, carefully read and understand the safety information, warnings, precautions, and instructions for proper operation of the CliniMACS Prodigy provided in the instructions for use of the CliniMACS Prodigy System components and in any safety-related recommendations issued by Miltenyi Biotec. These instructions for use include, without limitation, the safety information in the CliniMACS Prodigy user manual (instrument), chapter 3 'Important safety information'. Pay special attention to all warnings shown on the instrument or provided with consumables and accessories as well as notifications and important information described in this user manual. Adhere to all instructions and procedures at all times during the operation of the instrument, confirming that all safety information, warnings, precautions, and instructions are observed. Failure to follow the safety and important information, warnings, precautions, add notifications and instructions contained in the instructions for use could result in instrument malfunction, property damage, personal injury, and/or death. Equipment safety may be compromised if the instrument is not used according to the manufacturer's instruction. Retain the instructions for use 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 for all personnel responsible for installation, operation, and maintenance.

Table of contents

1 Introduction

1.1 General information

The software on the CliniMACS Prodigy includes core software and various application software.

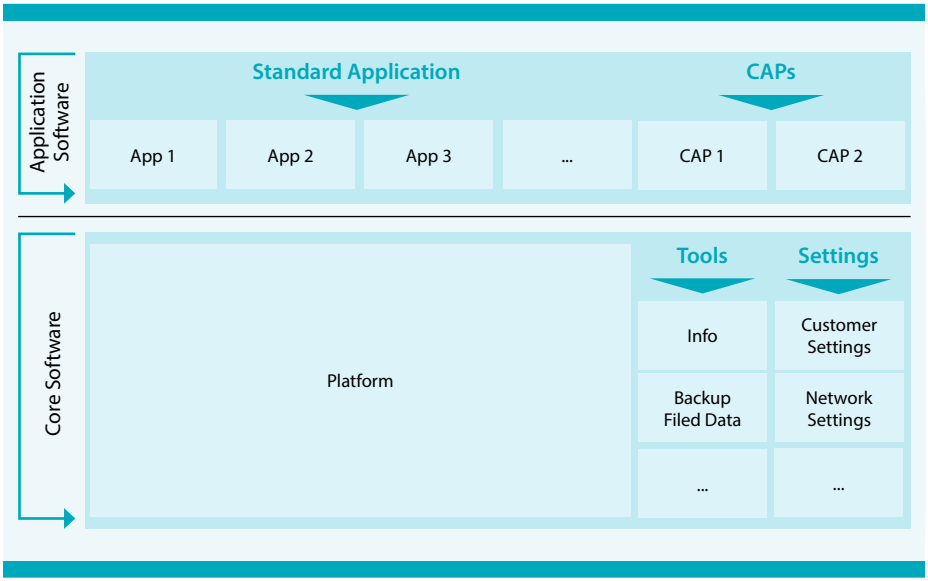


Figure 1.1: Overview of instrument software

The core software controls the instrument and execution of application procedures and provides essential services as described in the different 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 procedures and user interfaces for the operation of the CliniMACS Prodigy depending on its intended use:

- as part of the CliniMACS Prodigy Cell Separation System to separate human cells
- as part of the CliniMACS Prodigy Cell & Gene Therapy Manufacturing System for genetic and/or other substantial manipulation (like proliferation, differentiation) steps of human cells

The core software and each application are independent entities allowing a separate update of a new application without changing the core software.

1.2 Regulatory information

The software is developed according standard IEC/EN 62304. In addition, the CliniMACS Prodigy 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 including its penetration testing performed by a third-party company.

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

1.3 Data protection laws

When processing personal data with the CliniMACS Prodigy 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 has implemented security measures, especially the Defense-in-depth concept (see section 4.1 ´Defense-in-depth concept for security´).

1.4 About this manual

This user manual provides the required information for setup and safe operation of the core software. Only the core software 2.2 is within the scope of this user manual.

1.5 Associated documents

CliniMACS Prodigy Instrument user manual describes the CliniMACS Prodigy Instrument hardware and system. The instrument user manual is provided together with this manual.

The instrument user manual includes:

- Warnings, precautions, notifications
- Regulatory information
- Technical data
- Other important information

If using the CliniMACS Prodigy together with the MACS® TubeSealer, the CliniMACS Electroporator, the CliniMACS Formulation Unit, or the CliniMACS Workbench, consider these associated user manuals:

- MACS TubeSealer user manual
- CliniMACS Electroporator user manual
- CliniMACS Formulation Unit user manual
- CliniMACS Workbench user manual

A complete overview of the available accessories, components, and MACS GMP Instruments can be found in the CliniMACS Prodigy Instrument user manual.

For information regarding specific applications, contact Miltenyi Biotec Technical Support.

2
Glossary

2.1 Hazard level

The color and signal word of a warning message depend on the hazard level. The hazard level classifies the hazard, as described below. The level, type, and source of the hazard, as well as potential consequences, prohibitions, and measures are indicated 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 information considered important, but not hazard-related (e.g., messages relating to property damage).

IMPORTANT

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

2.2 Presentational conventions

Text in **<light green>** indicates elements in the graphic user interface (e.g., buttons, dialog boxes or user management items).

2.3 Glossary of symbols and terms

An overview of symbols and general terms used for the CliniMACS Prodigy System is provided in the CliniMACS Prodigy Instrument user manual. The glossary of symbols depicts the symbols used for labeling of the CliniMACS Products.

2.3.1 Software-specific terms

Application process	Software for cell processing developed by Miltenyi Biotec
ATS Audit Trail System	A software component that tracks and records the events, actions, user inputs, and changes made within the CliniMACS Prodigy Software
CAP	Customized Application Process
FTP File Transfer Protocol	Standard communication protocol used for the transfer of computer files from a server to a client on a computer network
LDAP 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
SMB Server Message Block	Communication protocol used to share files, printers, serial ports, and miscellaneous communications between nodes on a network
SMTP Simple Mail Transfer Protocol	Communication protocol for electronic mail transmission
Standard application process	A pre-validated application process provided by Miltenyi Biotec
UMS User Management System	A software component to manage and control user access to the various functions on the instrument

3

Important safety information

3.1 Safety instructions for the CliniMACS Prodigy

For detailed information regarding safety of the instrument refer to CliniMACS Prodigy Instrument user manual.

3.2 Safety instructions for the software

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 10 ´User management´). In case of failed login during a process run, contact Miltenyi Biotec Technical Support.

- Before using the instrument with software version 2.2, read the chapter 3 ´Important safety information´ in the CliniMACS Prodigy user manual (instrument) and all other information contained in this software user manual, including any safety 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 Provider should install, maintain, or service the instrument.
- The communication and data access between the software and 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.

4

Cybersecurity

4.1 Defense-in-depth concept for security

Cybersecurity is a shared responsibility between Miltenyi Biotech and 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 use, a defense-in-depth model is recommended. The goal of this defense-in-depth model are:

- Preventing negative impact on cell product quality and delay of cell product
- The integrity of protocols, processes, and audit data
- The integrity of the device 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:

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

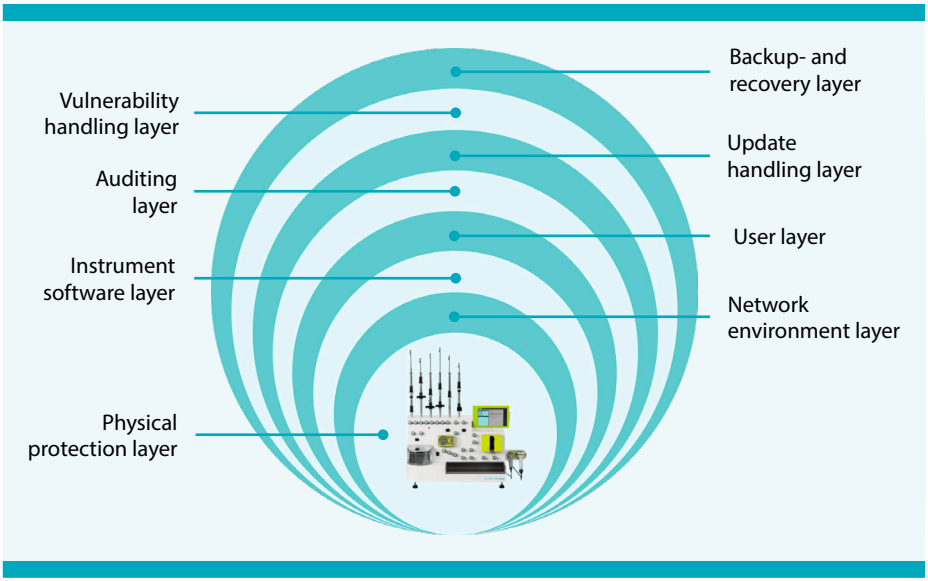


Figure 4.1: Layers of the defense-in-depth concept

4.1.1 Physical protection layer

The instrument is equipped with the following physical interfaces which support the connection of the different components, accessories, and instruments (see Table 4.1). 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
USB port	Connect approved peripherals to the instrument, such as the External Keyboard or the Barcode reader. A USB-Ethernet connector can be used to connect the instrument to the network. USB flash drives can be used for transferring protocols, images, and log files from the instrument and bringing programs/updates to the instrument as well as for the installation of the instrument
Touchscreen	A data input device used by maintenance and service personnel as well as operators.
CAN bus/power CAN interface	The interface allows the connection of the instrument to additional devices, such as the CliniMACS Electroporator or the CliniMACS Formulation Unit.
Tube sealer connector	Provides power to the MACS TubeSealer, a heat sealer installed on the CliniMACS Prodigy. No data interface.
Alarm connector	Relay circuit connector for the connection of the instrument to an external alarm system. No data interface.

Table 4.1: Interfaces and peripherals of the instrument

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.

Note: Only FAT32 format USB flash drive is supported.

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

4.1.2 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 4.2. A router separates the different network segments from each other and controls the data flow between them.

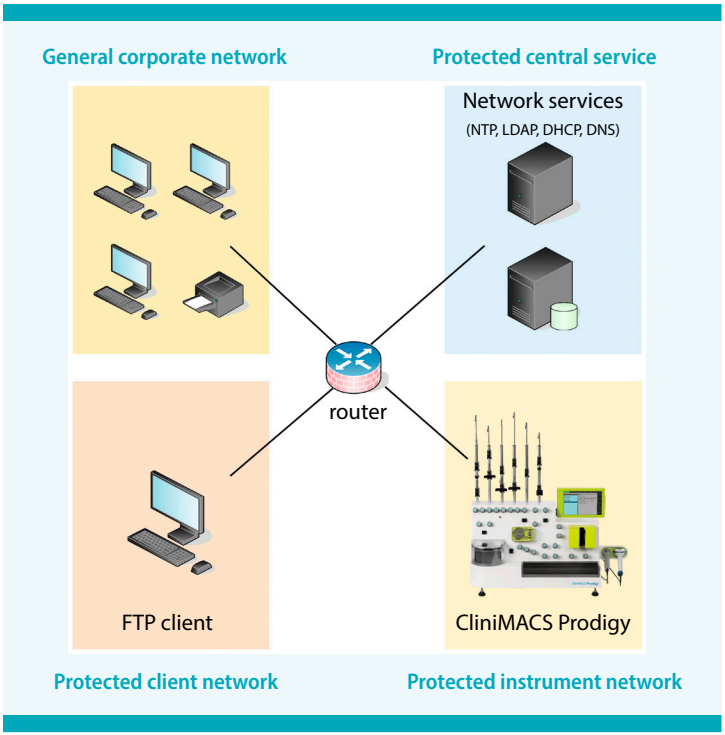


Figure 4.2: Network diagram

The instrument mainly provides functions to connect to other systems on the network. The supported network protocols are listed in Table 4.2.

Interface	Purpose	Port	Comment
FTP	Read-only log file access via FTP	20 – 21	Using FTP transmits the log files and passwords in clear text over the network. It is recommended to use a dedicated user account for accessing data via FTP to limit the risk to the FTP service and prevent lateral movement in case the user account becomes compromised.By default the FTP is disabled.
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 9.2 ´Connecting to an LDAP server´.
SMB	File Sharing	445	Authenticated share is supported. Requires configuration, see section 9.3 ´Connecting to a network drive´
SMTP	Email notification	25, 2525, 465, 587	Authentication is supported, Requires proper configuration, see section 9.5 ´Connecting to an email server´
SMTPS	Secured version of SMTP	465, 587	A secure variant of SMTP. Requires proper configuration, see section 9.5 ´Connecting to an email server´

Table 4.2: Network connections and protocols

IMPORTANT

Except for FTP, secure protocols are supported for all services. It is strongly advised to only activate the secure functions listed in Table 4.2. 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.

4.1.3 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 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 an operator 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 'injected', i.e., 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 below in section 4.1.6 ´Update handling layer´.

New instrument software versions, or customized application software are installed by Miltenyi Biotec Technical Support.

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 operator. 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 operator 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 procedures is available to Miltenyi Biotec Technical Support only and in normal operations not available to the customer. Access is available to users logging in with the service account or with a service USB flash drive, i.e., a USB flash drive with authentication information, and associated PIN or through the remote access functionality of the Info tool in combination with a one-time PIN provided by Miltenyi Biotec. Only Miltenyi Biotec Technical Support has access to the credentials for the service account and the service USB flash drive. A one-time PIN may be provided by technical support for use during remote support cases.

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.

4.1.4 User layer

All access to the component can be protected via configurable 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.

4.1.5 Auditing layer

The audit trail system logs information about actions performed on the instrument, e.g., operator 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 (e.g., export, storage, deletion, and review) of audit trail data following applicable regulations.

4.1.6 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 Technical Support only. The instrument software updates are delivered and installed following procedures outlined in Miltenyi Biotec's SOPs. Updates are packaged in dedicated packages containing the new instrument software as well as 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 this is checked before installation. Contact Miltenyi Biotec Technical Support for scheduling an update of the instrument.

4.1.7 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 11 ´Troubleshooting´).

4.1.8 Backup- and recovery layer

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

4.1.9 Summary of secure configuration

The previous sections introduced security measures that are in place and recommend measures to set up for the secure operation of the CliniMACS Prodigy. These measures fall into the domains of the configuration of the instrument and procedures and policies that add to the security of the instrument. The following measures are recommended:

- Ensure that only authorized personnel have physical access to the instrument and its physical 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 where the instrument supports them.
- Because of the missing encryption of FTP traffic to and from the instrument, it is recommended to set up and use a dedicated user for accessing data via FTP.
- 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 are made regularly and follow applicable regulations.
- It is the customer's responsibility that no personal health information is used on the instrument.

5 Software concept

5.1 Basic concept

The software running on the instrument is composed of the 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.

Application process

A standalone software represents a biological process, e.g., T Cell Transduction Process or LP-34 Enrichment. 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. There are two types of application process:

- Standard Application Process: A pre-validated application process provided by default.
- Customized Applications Process (CAP): A bespoke application process developed for dedicated customers.

Tool

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.

Setting

An executable program to configure the instrument. For instance Network Settings, Customer Settings, and Module Settings

For each executable program, a folder, which contains all information will be created. The folder is named by [Date]_[Time]_[SerialNumber]_[ExecutableProgram].

The content of this folder is controlled by the executed program. For application processes, the customer-relevant files are listed in Table 5.1.

File/Folder name	Description	Format
Protocol.pdf	Electronic record of application run	.pdf
Prototol_ Appendix_I.pdf	Error and warning log during application run	.pdf
Interphase	Interlayer camera images	Folder
Microscope	Microscope images acquired during application run	Folder
checksums.md5	Checksum	.md5
IR_Monitor	Logs the time and temperature when chamber surface temperature out of specification during cell culture	.html

Table 5.1: Log files of application processes

5.2 The graphic user interface

The graphic user interface (GUI) contains several sections: menu bar (with quick access menu), toolbar, status line and content area (Figure 5.1). During software operation, GUI elements and content change based on the activity and process.

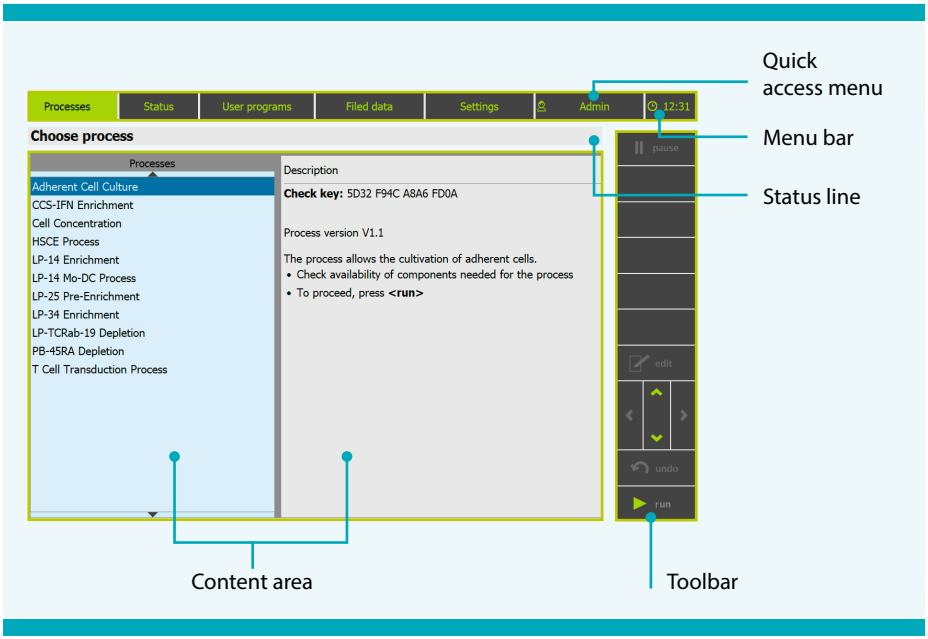


Figure 5.1: Sections of the graphic user interface

5.2.1 Menu bar and content area

The menu bar provides access to <Processes>, <Status>, <User Programs>, <Filed data>, <Settings>, and (quick access menu). A green background indicates which menu button is active. Tap in the respective area to activate the menu. The content area adapts according to the selected menu. Upon login, <Processes> is selected by default and the content for processes is shown (see Figure 5.1).

Menu	Description
<Processes>	Access to standard application processes installed on the instruments (Screen 6.5) and guides through the process run (Screen 6.6)
<Status>	Instrument status during an application process run (Figure 6.1)
<User Programs>	Access to Miltenyi Biotec Customized Application Process (CAP) and guides through the process run
<Filed data>	Access to viewing and exporting data generated from processes, tools, and settings (Screen 7.1).
<Settings>	Access to settings and tools for instrument configuration, function test and basic troubleshooting (Screen 8.1)
Quick access menu	Access to logout, user management, password policy, audit trail and shutdown button (Screen 6.3)
System time:	Current system time.

Table 5.2: Menus in the menu bar

5.2.2 Status line

The status line (see Figure 5.1) contains brief information regarding the status of the current process.

5.2.3 Toolbar

The toolbar contains various buttons to control the process. The availability of the buttons and the active status of the buttons are controlled by the application process. Figure 5.2 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 5.3.

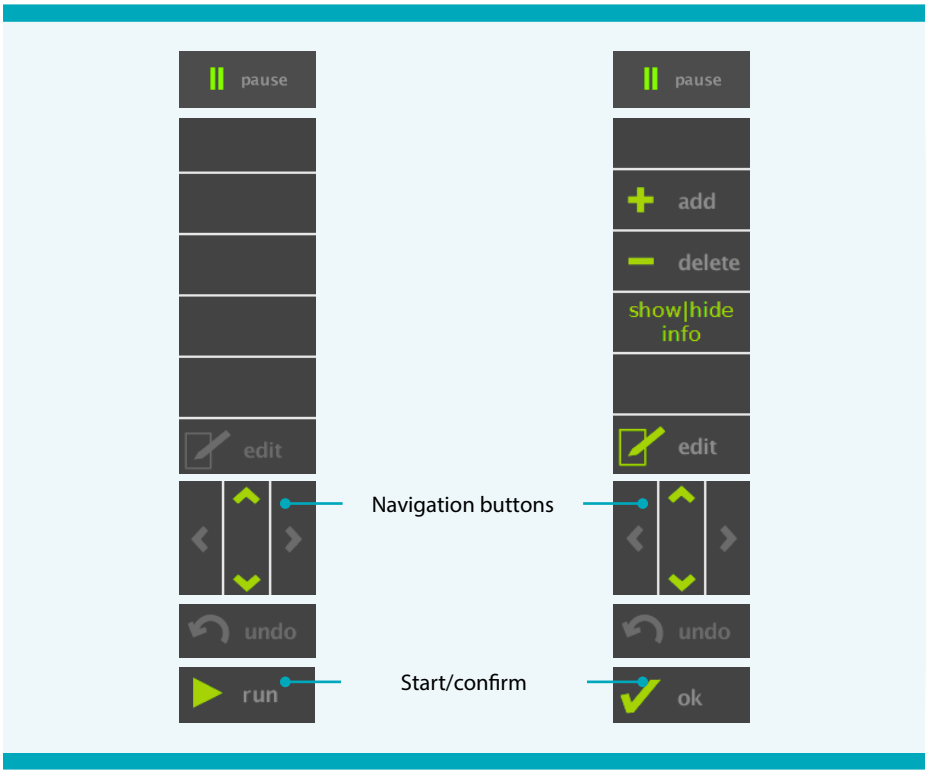


Figure 5.2: Dynamic and static buttons of the toolbar

Button name	Description	Availability
<pause>	temporary halt/suspension of the currently running process, depends on the running application	during a process run
<edit>	activates the input field for manual data input (see 5.2.4 ´Input fields´).	if input fields are available
navigation buttons	to select elements from a list: use ^ v to move selected item up and down in the list (see Screen 6.5) or < > to switch between lists (see Screen 8.1). to navigate in images from the camera (Figure 6.3).	always if the camera is active
<undo>	revokes one or more inputs to restore the original content of the screen	during a process run
<ok>/<run>	<ok> confirms a selection or closes the active menu <run> starts a process, user program, or any other procedure	always

Table 5.3: Frequently used buttons in the toolbar

5.2.4 Input fields

An input field represents a keypad and allows for the input of letters or numbers (see Figure 5.3). For manual entry of capital letters, tap <⇧>, for space tap <SP>, for numbers tap <?123>, and for backspace tap <⌫>. To open the input fields, tap <edit> in the toolbar. To close the input field, either tap <ok> at the bottom of the input fields to confirm the input or tap <Escape> on the top-right to close without saving.

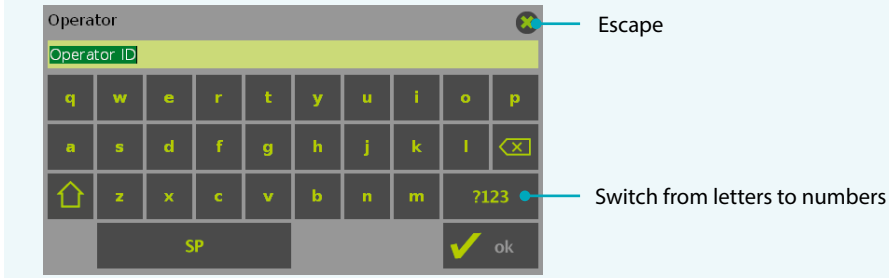
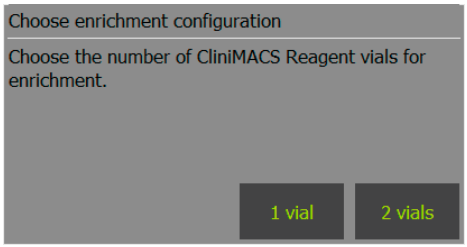


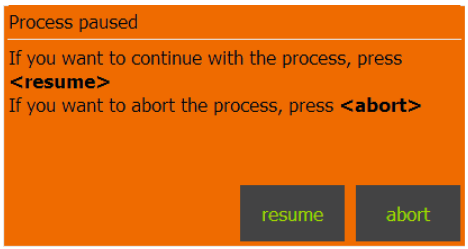
Figure 5.3: The input field – keypad with letters

5.2.5 Pop-up windows

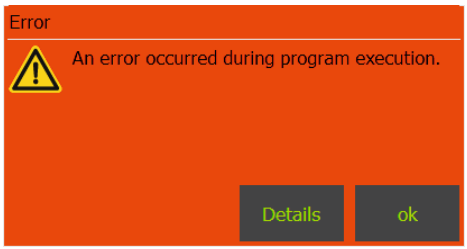
Pop-up windows might be shown while running executable programs. The running process will be interrupted until the pop-up window is closed. If necessary, the pop-up windows can be dragged around the screen while holding the top bar. There are several scenarios when a pop-up is shown:



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



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



An error occurred. The pop-up window shows a red background. Select one of the buttons on the bottom to continue.

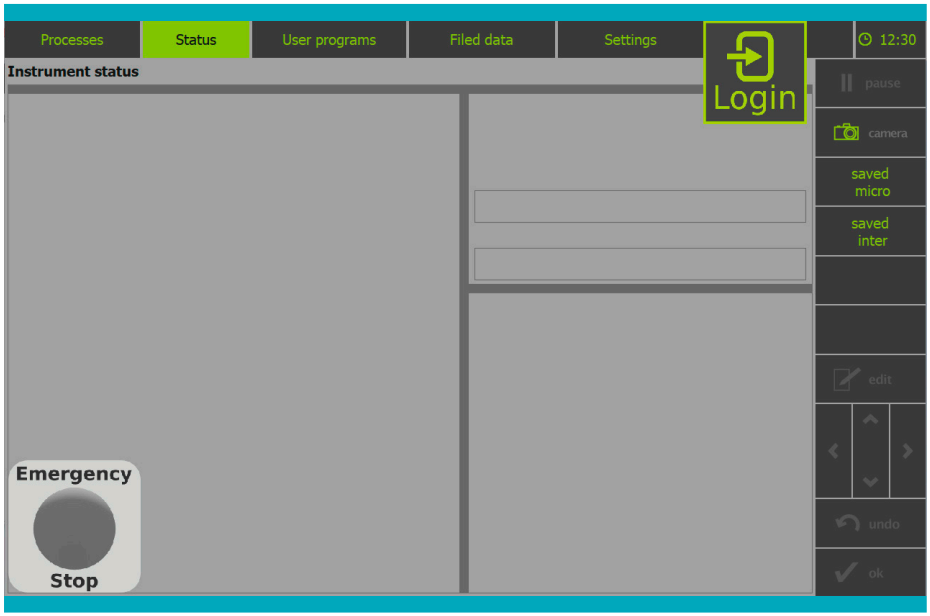
If required, contact Miltenyi Biotec Technical Support

6

Basic operation

6.1 Switching on the instrument

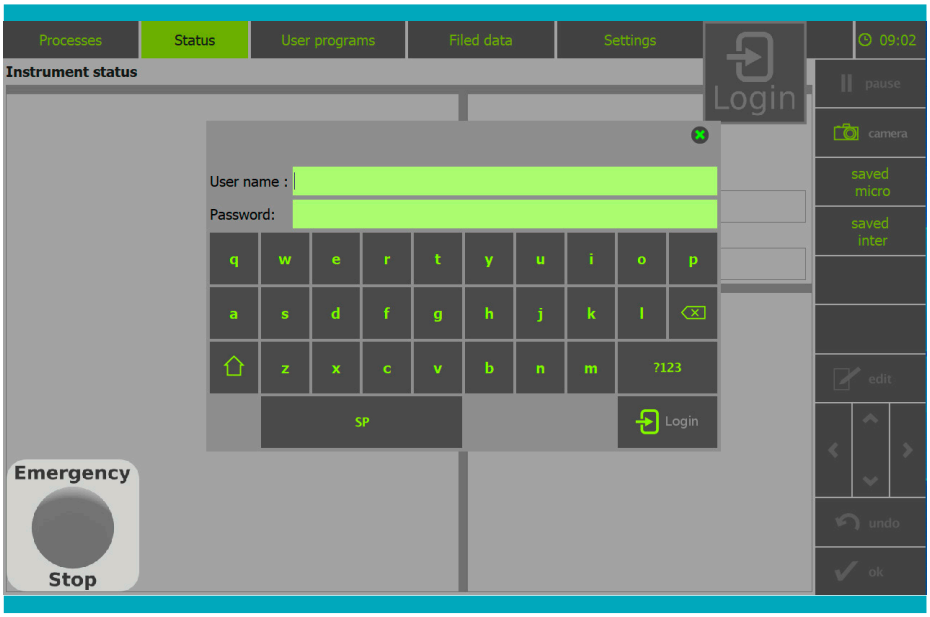
Switch on the CliniMACS Prodigy with the power switch located on the rear side of the instrument. The start screen shows the software version and initialization process appears for a short time (approx. 5 seconds). After the initialization process, a locked screen will appear (see Screen 6.1). Only the <Login> button is activated on this screen.



Screen 6.1: Locked screen

6.2 Login

Tap <Login> in the upper right corner of the screen to open the pop-up window <User Login> (see Screen 6.2). Enter username and password and tap <Login> within the pop-up window. The screen will unlock. The username and password should be setup before use (see chapter 10 ´User management´for details).



Screen 6.2: User login window

Note: In case of login failure, contact a system administrator to verify:

- Correctness of username and password.
- Access rights of this account. For more information, see chapter 10 ´User management´.

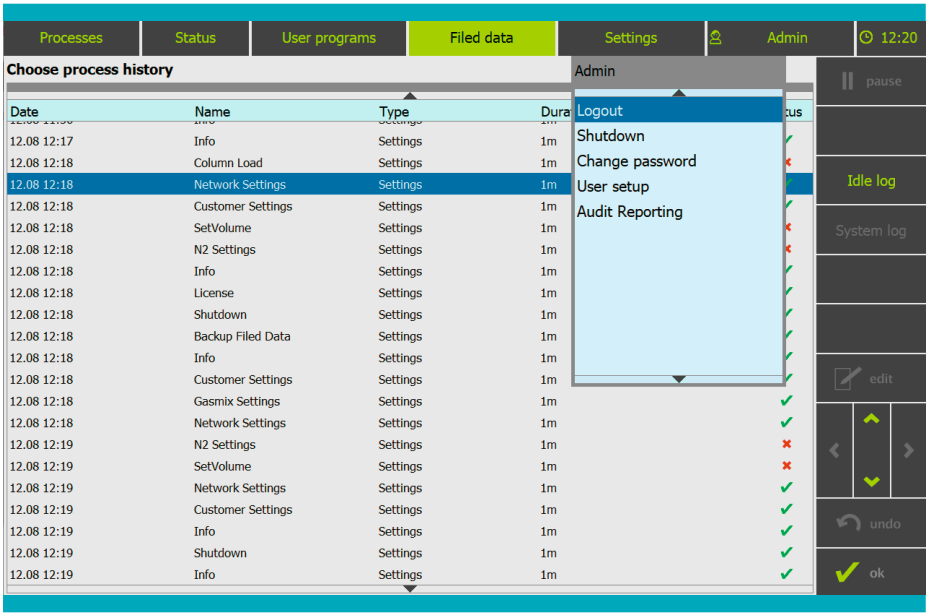
If a pop-up notification appears during login that is not related to incorrect user credentials or missing access rights, tap <ok>. Then, enter the user credentials again.

If login still fails, contact Miltenyi Biotec Technical Support.

6.3 Logout

Tap (quick access menu), and select < Logout> from the list (see Screen 6.3). The screen will then be locked again.

Note: After 20 minutes without interaction with the software the user will be logged out automatically.



Screen 6.3: Logout

6.4 Shutdown

Tap (quick access menu). Select <Shutdown> from the list (see Screen 6.3). Alternatively, go to <Settings> ▸ <Tools> ▸ <Shutdown>. Wait for the shutdown process to finish, and then switch off the instrument using the power switch located at the rear side.

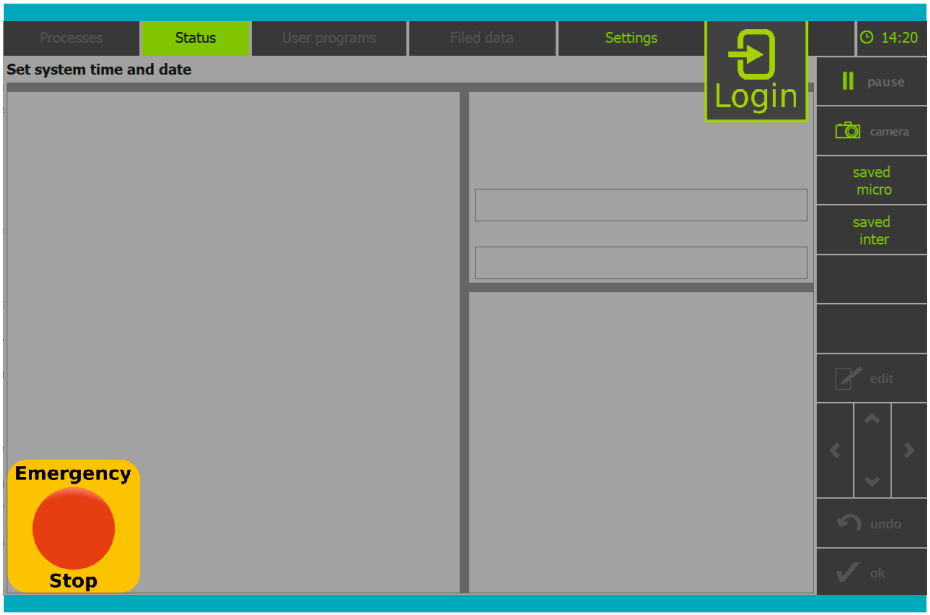
6.5 Emergency Stop

<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 is only activated (indicated by the colors yellow and red) when an application or a tool is running and no user is logged in (see Screen 6.4).

IMPORTANT

The <Emergency Stop> 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.

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



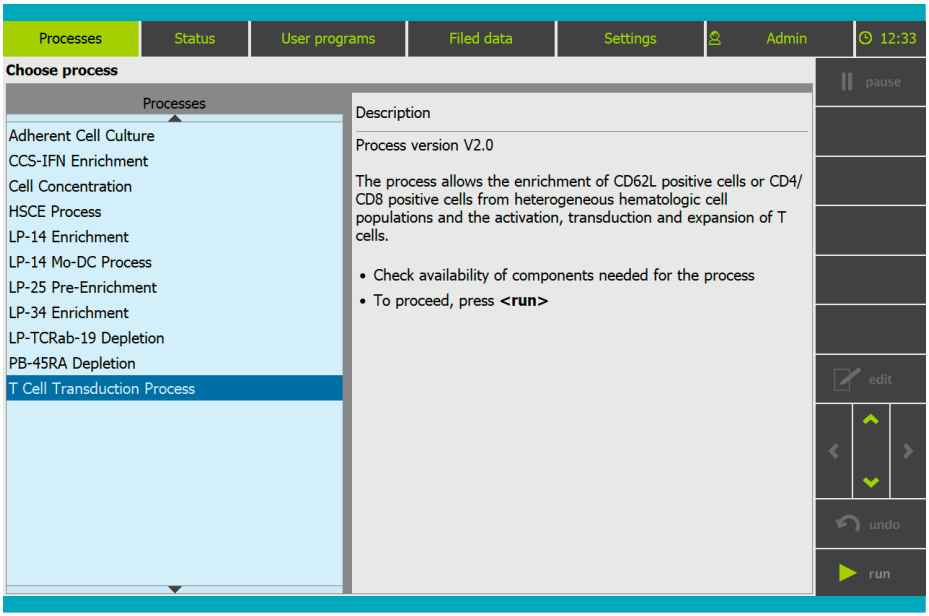
Screen 6.4: Emergency Stop button

6.6 Select an application process

1. Tap <Processes> in the menu bar for a standard application process. For a CAP tap <User Programs>.

2. Select the desired process from the process list (Screen 6.5). Selected process is highlighted with blue background. Description of the application can be found on the right. Tap and in the process list or use ^ and ⌄ on the toolbar to navigate button through the available processes.

Note: 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. More information regarding roles and right, see chapter 10 ´User management´.



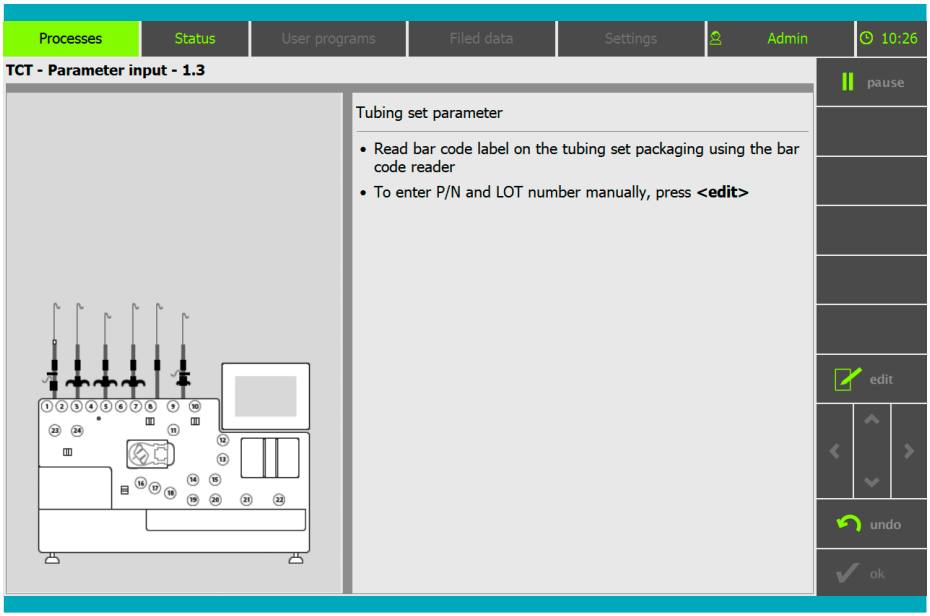
Screen 6.5: Select an application process

6.7 Execute an application process

To start the process, select a process and tap <run> in the toolbar. The software provides step-by-step guidance through the process. Screen 6.6 shows an example step of the TCT application. The status line shows the current step name and index. The content area gives more information on the respective step. Follow the illustration and instructions in the content area for each step.

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 barcode scanner or manually. For manual entry or if barcode scanner input is not accepted, tap <edit> in the toolbar and use the input field.

When all required actions are completed, <ok> in the toolbar will be enabled. To go to next step, tap <ok>. To go to the previous step, tap <undo>.



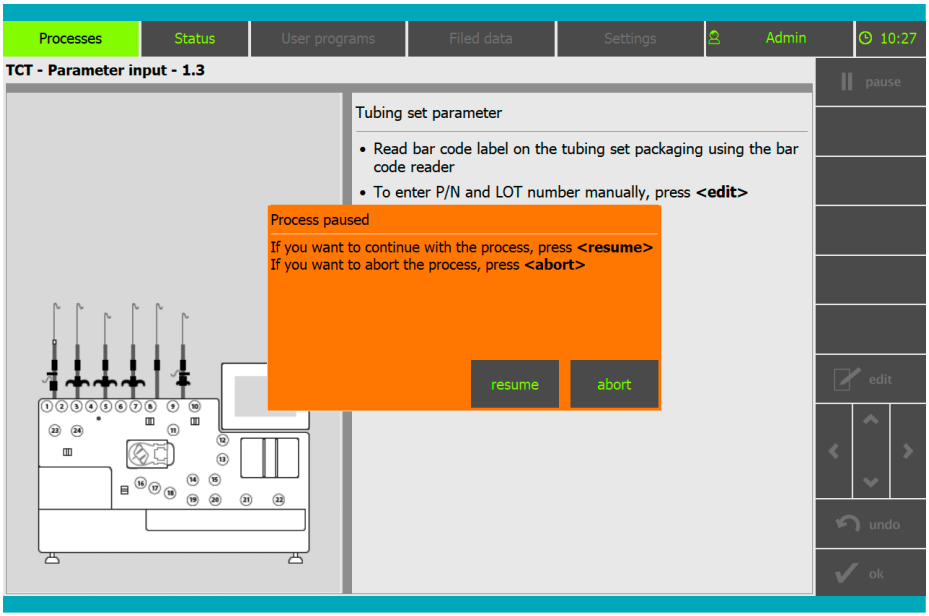
Screen 6.6: Example step in the TCT application process

6.8 Pause an application process

To pause the current process, tap <pause> in the toolbar. A pop-up window will appear (Screen 6.7). To continue a paused process, tap <resume>. To end the process, tap <abort>.

IMPORTANT

An aborted process cannot be resumed.



Screen 6.7: Process paused

6.9 Instrument and application process status

To check the operational state of the running process, tap <Status> in the menu bar. The content area shows the following elements:

- Process-related parameter: a list of all relevant process parameters (see Figure 6.1, left).
- Info box and progress status: process-related information (see Figure 6.1, top right):
  - Operator name
  - Sample information
  - Subprocess progress and remaining time
  - Process progress and remaining time before next user interaction
- Graphic overview: provides visual information about the running subprocess status of the instrument (see Figure 6.1, lower right). All activities of the instrument components (e.g., peristaltic pump, pinch valves) are visualized in orange.

Note: Status information is only available during an application run. This page is blank when no application is running. Graphic overview might not be available for CAPs.

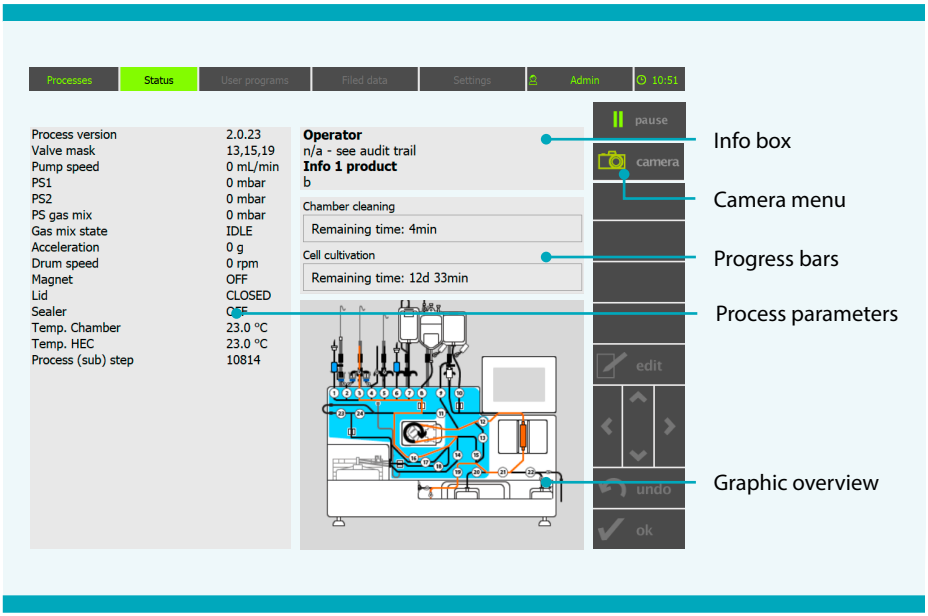


Figure 6.1: Overview of instrument status

6.10 Acquiring images

Two camera functionalities can be selected with <camera> in the toolbar during selected applications (see Figure 6.1).

- Layer Detection Camera image: This image is used to measure the volumes of the centrifugation fractions. It is only available in selected applications and only for selected applications and during the first volume adjustment after sample loading after sample loading (see Figure 6.2).
- Microscope image: This image can be used to visually monitor cell culture. It is only available during cell culture procedures (see Figure 6.3).

The image will be automatically captured and saved to the protocol by the application process. To view images, tap <camera> in the toolbar when <Status> menu is selected (see Figure 6.1). Depending on the step of the application process, the content area will show either a layer detection camera image or microscope image.

Note: The availability of <camera> in the toolbar is controlled by the application process. Images will be recorded automatically during an application.

6.10.1 Layer Detection Camera

The different layers are automatically detected by the software. In Figure 6.2 red and orange bars mark the position of the layers within the image. A diagram below the image shows the recorded values for the volumes of the centrifugation fractions. The curves are shown in red and orange corresponding to the bars within the image (see Figure 6.2).

Figure 6.2: Overview of instrument status

The following functionalities are supported:

- Image recording: Tap <snap> in the toolbar. After a short recording phase (approx. 15 seconds), the shown image will be replaced by a newly recorded image.
- Image archiving: Tap <save> in the toolbar. The recorded image will be integrated in the protocol of the current process.
- Quitting camera menu: Tap <ok> in the toolbar.

Note: The availability of the buttons above is controlled by the application process.

6.10.2 Microscope camera

The camera menu shows the last image saved by the integrated microscope camera (see Figure 6.3).

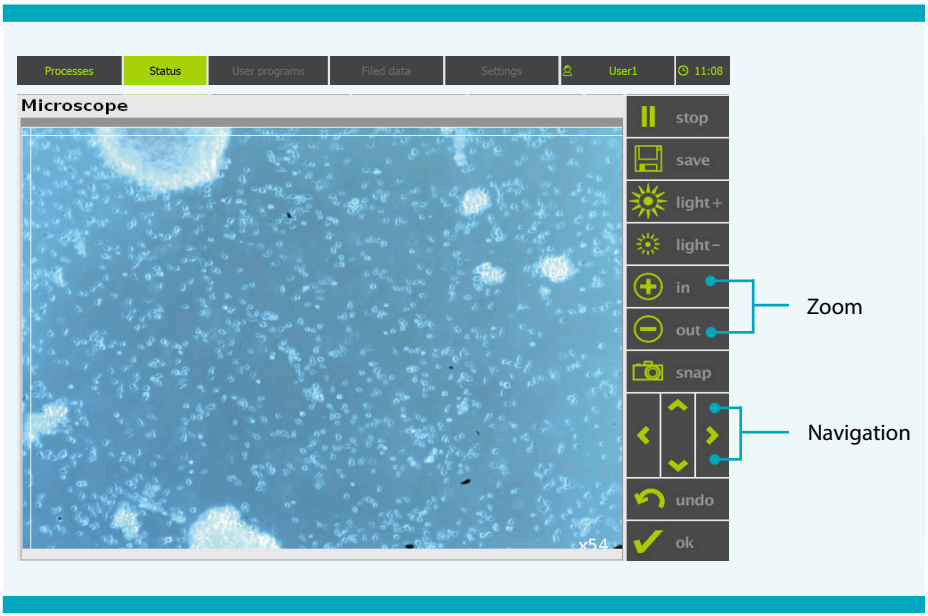


Figure 6.3: Status screen when microscope camera is active

The following functionalities are supported:

- Zoom image: Touching the image of the microscope camera will result in a 2-times magnification. The point of touch will be the new center of the image. The magnification of the images is up to 400-fold.
- Navigation within an image: Tap a navigation button to shift by half a frame in the selected direction. Image scroll bars show the absolute position of the image section in the whole image to facilitate the navigation. Tap <undo> repeatedly to undo the last ten navigation steps separately.
- Image recording: Tap <snap> in the toolbar. After a short recording phase (approx. 15 seconds), the shown image will be replaced by a newly recorded image.
- Image archiving: Tap <save> in the toolbar. The recorded image will be integrated in the protocol of the current process.
- Quitting camera menu: To quit the camera menu tap <ok> in the toolbar.

Note: The availability of the buttons above is controlled by the application process.

7 Data access

7.1 Retrieving application logs

7.1.1 Viewing and exporting log files to USB

<Filed data> menu shows the log file generated from the application processes, tools and settings. In the content area, file list shows the time, name, type, duration and status of the process run (Screen 7.1).

Note: The menu <Filed data> is not available during a process run. The respective touch button is inactive.

Viewing log files

To view the content of the process protocol PDF and protocol appendix PDF, select the target log and tap <ok> (see Screen 7.1). The content of the selected file will be shown in the content area (see Screen 7.2). To return to the file list tap <ok>.

Screen 7.1: Example list of filed data

Screen 7.2: Example of a process protocol (TCT application)

Export to 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 8.2.2 'Backup Filed Data'.
- The USB flash drive must be FAT32 format and should not be password-protected.

7.1.2 Retrieve via FTP

FTP is a network protocol that allows the transfer of data between the CliniMACS Prodigy (referred to as FTP server) and the end user's computer (referred to as FTP client) over IP (Internet Protocol) connections. All the log files generated from the application run can be accessed.

To access data via FTP, configuration is required. To setup the instrument for FTP connection, follow the instructions in section 9.4.1 'Setting the instrument'. After configuration, the user can connect to the instrument with any available FTP client (e.g., FileZilla) to download protocols and log files, Figure 7.1 shows an example of connection parameters. To connect to the instrument, enter the following information:

- The IP address of the instrument. It can be found under <Settings> ▸ <Tools> ▸ <Info> ▸ <Network information>.
- The port: Use standard port 21.
- For username and password two login options are supported:
    - Login option 1: A registered account in user management system (see chapter 10 'User management'). In this case, use the user login account and password. The connection establishment and termination will be recorded in the audit trail.
    - Login option 2: A local username and password saved in FTP/File Share Settings. The login info can be found under <Settings> ▸ <Network Settings> FTP/FS. In this case, connection establishment and termination will not be recorded in the audit trail.

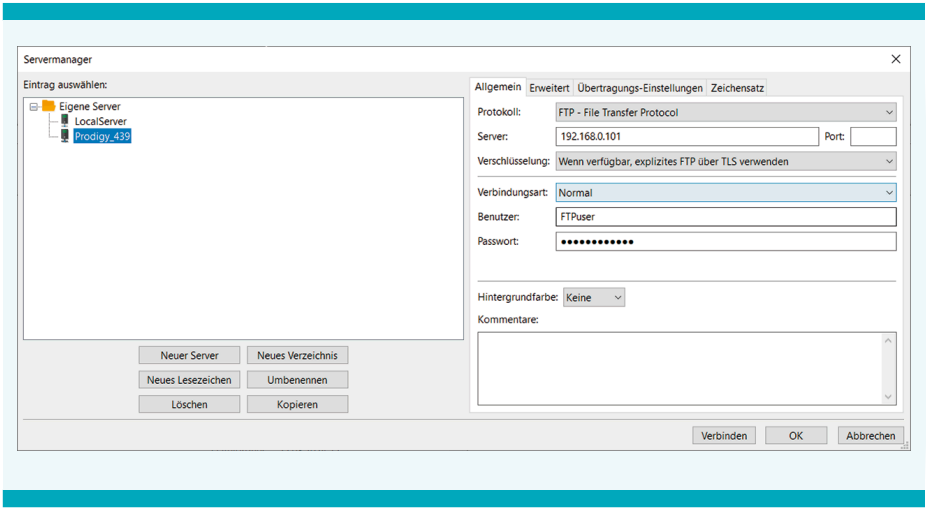


Figure 7.1: Exemplary connection parameters

- **IMPORTANT**
  If login option 1 is used, make sure 'File management user' role is assigned to this account. Regarding how to assign the role to account, check chapter 10 'User management'.
- The software does not support secured FTP (sFTP). It is recommended to use the instrument in segregated network if files are accessed via FTP.

Note: An individual user may only establish a single connection at a time, as multiple connections are not allowed by the instrument's server. If a client software is used that uses simultaneous connections (e.g., FileZilla) change the settings to the client accordingly to allow only a single session. Otherwise, the contents can only be browsed but not downloaded.

7.1.3 Retrieve files via File sharing

The log files generated during the application run can be retrieved via a shared network folder. Once the application run is complete, all generated files will be automatically placed in a subfolder created for each instrument within the shared folder. Figure 7.2 shows the file structure in the shared folder. To enable file sharing, configuration is required. For setup file sharing, follow the instructions in section 9.3 'Connecting to a network drive'.

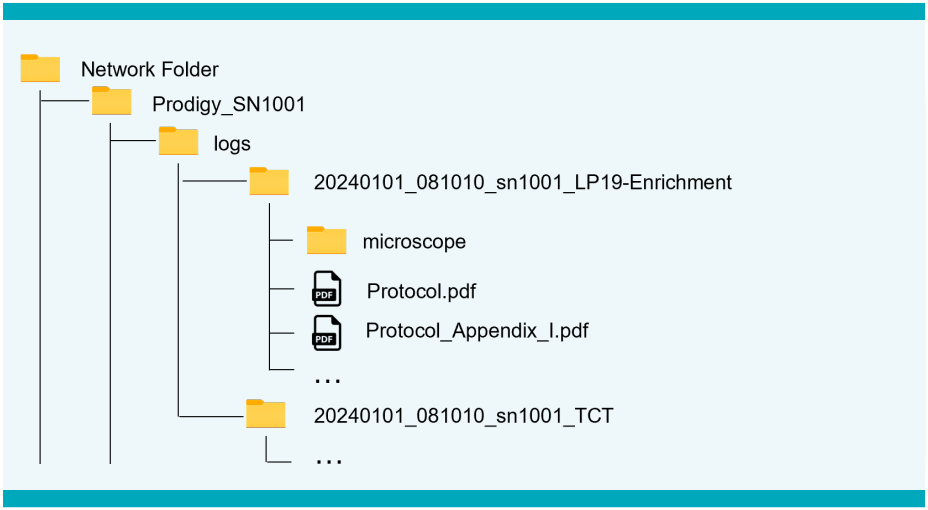


Figure 7.2: File structure in file sharing

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.

7.2 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 7.1 shows the audit trail format.

IMPORTANT

The timestamp of the audit trail record is always UTC time.

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

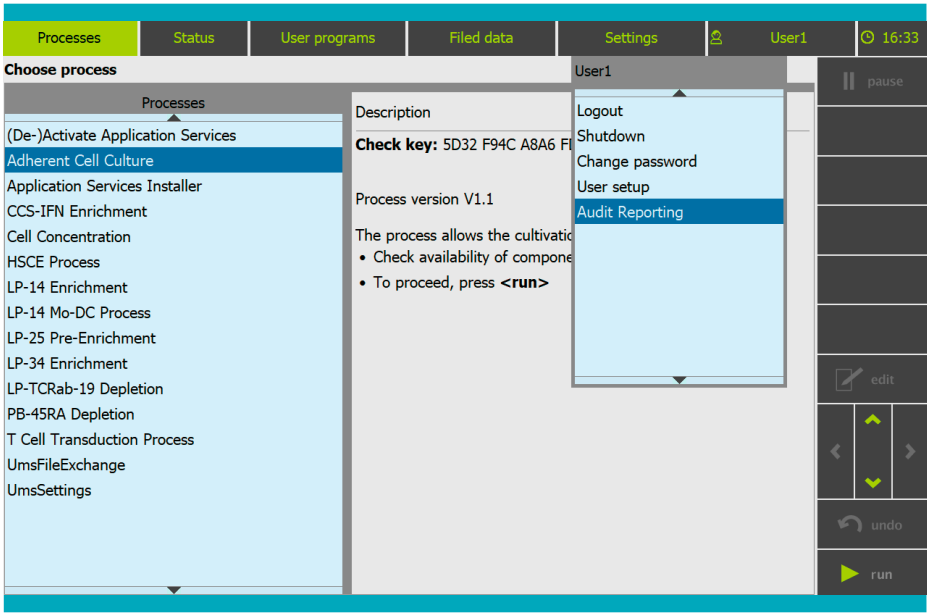
Table 7.1: Audit trail format

Note: 'ATS User' role or role with 'Audit Trail Management' rights is needed to access the audit trail system.

- '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 10 'User management' for more details on how to configure roles and rights.

7.2.1 Viewing audit trail

To open the Audit trail, go to ▸ <Audit Reporting> (see Screen 7.3). The <Audit Trail> menu contains a list of all available audit trail events on the instrument (see Figure 7.3).



Screen 7.3: Audit reporting

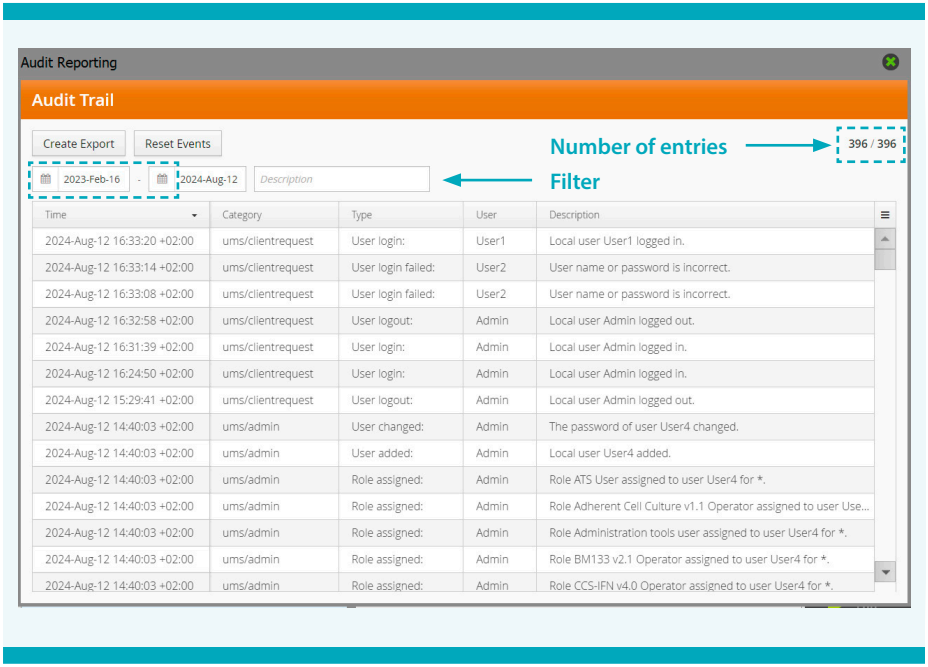
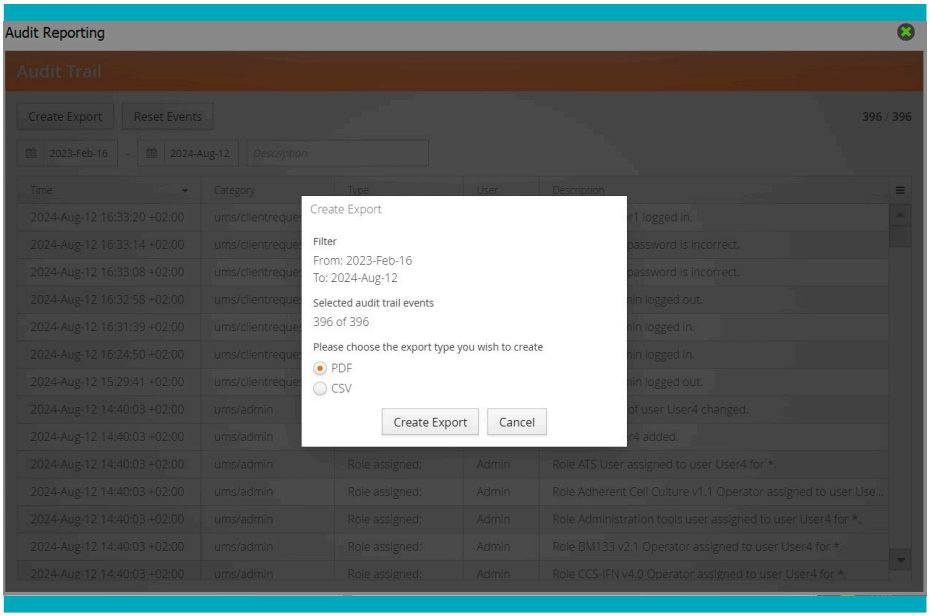


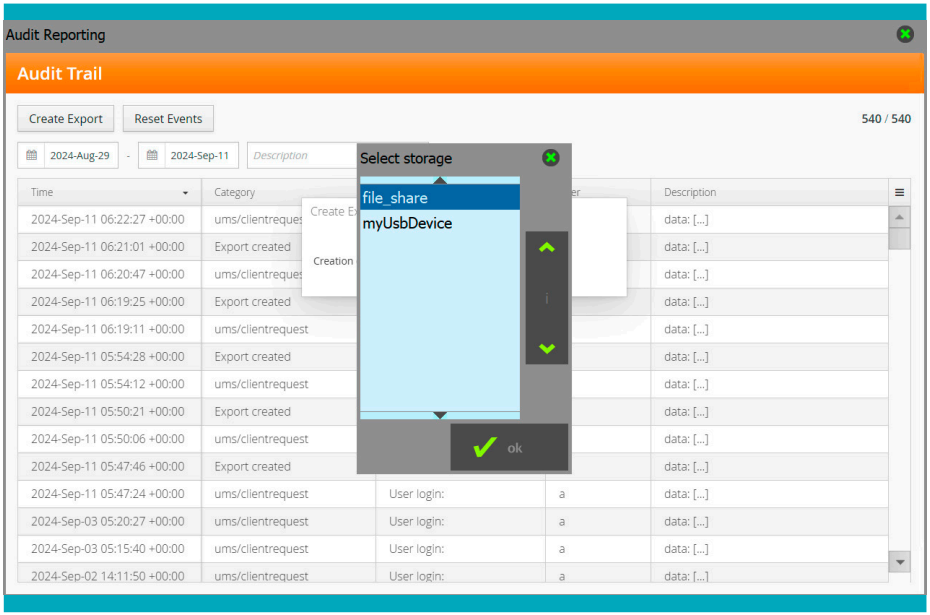
Figure 7.3: Audit trail menu

7.2.2 Exporting audit trail

1. Enter the filter criteria in the fields in Figure 7.3. If no criteria is entered, all the audit trail records will be exported.
2. Tap <Create Export> above the filter criteria. A pop-up window will be shown (Screen 7.4).
3. Choose the format and tap <Create Export> in the pop-up window.
4. If multiple storage locations are detected, e.g., file sharing is configured and a USB flash drive is inserted, the storage location needs to be chosen (Screen 7.5).



Screen 7.4: Create audit trail export



Screen 7.5: Select storage location for audit trail

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

7.2.3 Deleting audit trail

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.

IMPORTANT

It is not possible to delete single entries. Deleted data cannot be restored. Make sure only authorized users have the right to delete the audit trail. To configure roles and rights, see chapter 10 ‘User management’.

8

Tools and user settings

8.1 Access to tools and user settings

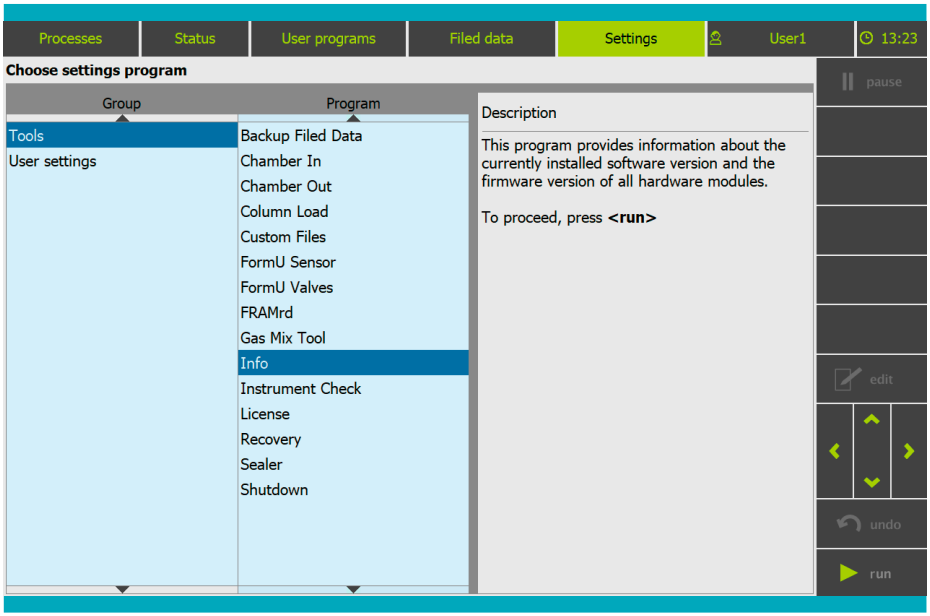
Two types of programs can be found in the <Settings> menu: Tools and Settings.

Note: Tools and settings are not available during a process run.

To find and run a tool/setting:

1. Select the <Tools> or <User settings> from the group list see Screen 8.1.
2. Tap on the desired program from the program list. The selected program is highlighted with a blue background. Detailed information about the selected tool/setting can be found in the description field. Tap ^ and v in the process list to browse through more options. Alternatively, use the navigation buttons to browse and select the program.
3. To start the selected program, tap <run> in the toolbar.

In the following sections, commonly used tools and user settings will be introduced.



Screen 8.1: Select a tool or setting

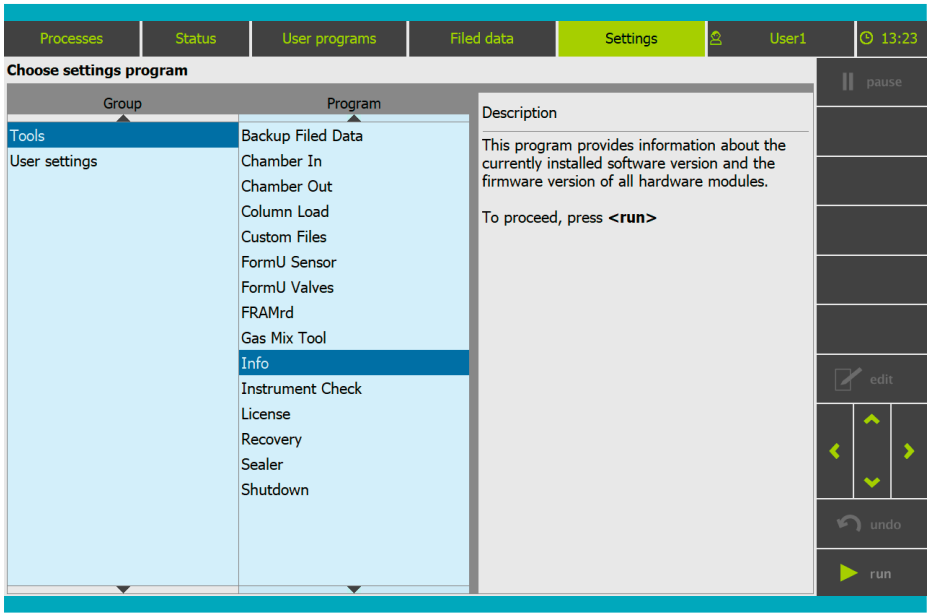
8.2 Tools

All tools can be found in <Settings> ▸ <Tools>.

8.2.1 Info tool

The Info tool provides detailed information regarding software and hardware. Important information includes:

- Software version
- Build number
- Firmware version
- Hard drive space usage, including remaining space, used space, total space
- IP address
- MAC address
- Complete runtime information (including all applications and tools), idle time (time the instrument was not running an application)



Screen 8.2: Info tool

8.2.2 Backup Filed Data

The Backup Filed Data tool copies all the process data to a backup location or deletes all process data.

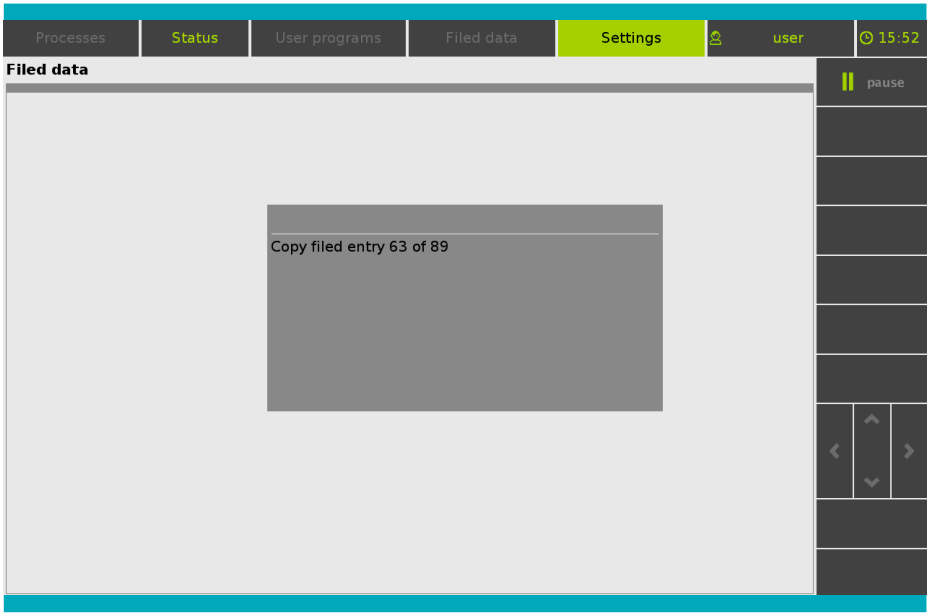
IMPORTANT

- It is recommended to backup the process data regularly. 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 FAT 32 and should not be password protected.
- If file sharing is configured files can also be exported to the file sharing folder (see section 9.3 ´Connecting to a network drive´).

Copy data

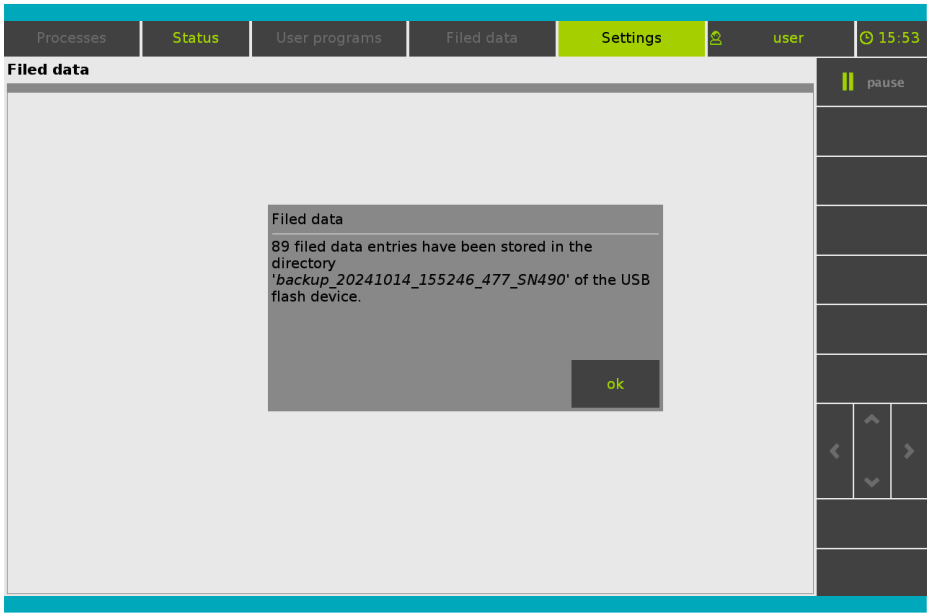
1. Insert a USB flash drive.
2. Go to <Settings> ▸ <Tools> ▸ <Backup Filed Data>, and tap <run>.
3. Select <Backup> on the prompt (see Screen 8.3). Copying will start (see Screen 8.4).

Screen 8.3: Select backup



Screen 8.4: Backup process

4. Wait until copying is finished, then tap <ok> on the prompt (see Screen 8.5).
5. Verify that the files have been downloaded completely.



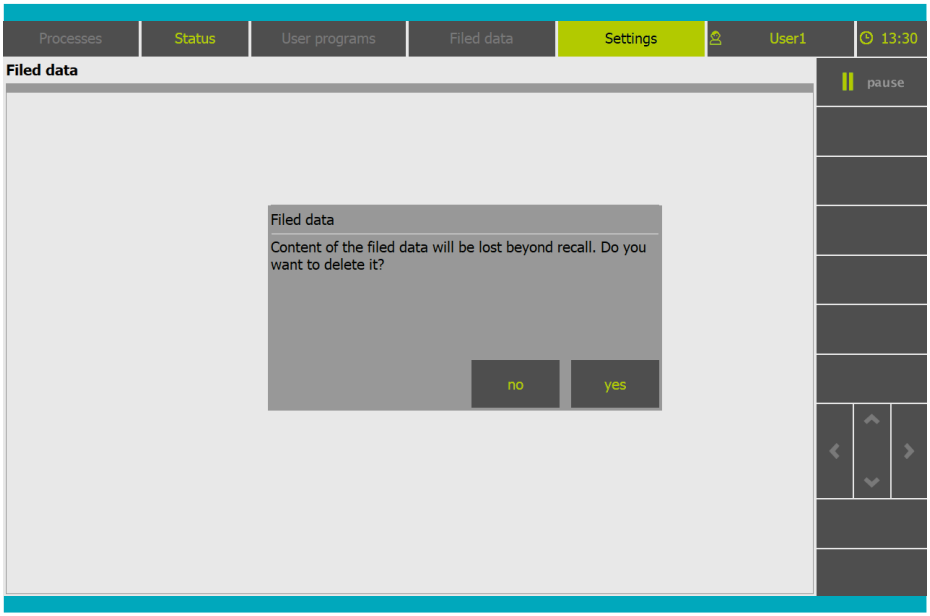
Screen 8.5: Backup completed

Delete data

1. Verify that the files have been downloaded completely.
2. Go to <Settings> ▸ <Tools> ▸ <Backup Filed Data>, and tap <run>.
3. Tap <Delete> (see Screen 8.6).

Screen 8.6: Select delete

4. To confirm, tap <yes> (see Screen 8.7).

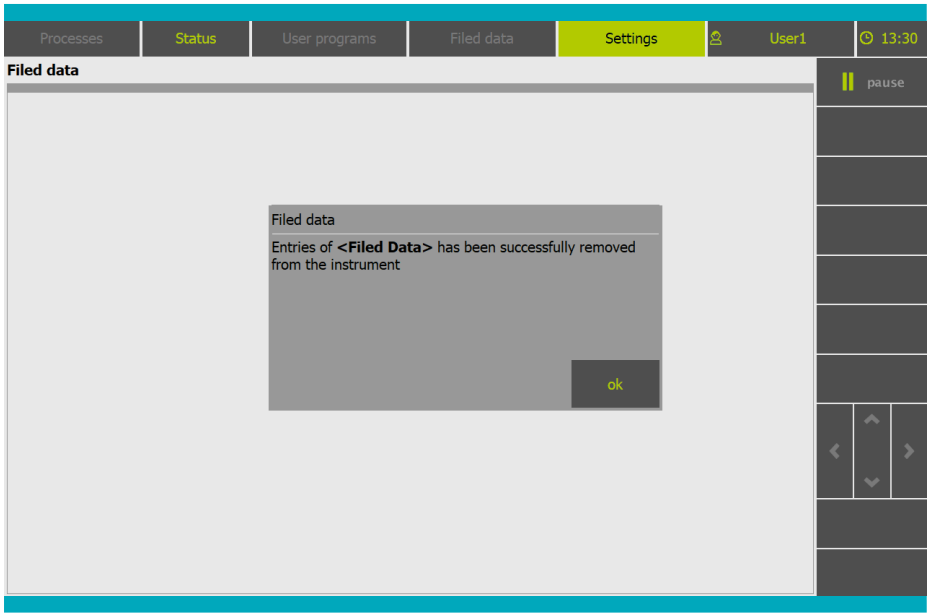


Screen 8.7: Confirm deletion of data

5. Wait for the deletion process to complete, then tap <ok> on the prompt (see Screen 8.8).

6. After deletion all records from <Filed data> will be deleted. One record for executing Backup filed data tool will be created.

IMPORTANT
Deleted data cannot be recovered.



Screen 8.8: Deletion complete

8.2.3 Chamber In

This tool is used to insert the CentriCult Unit outside of a running application. The chamber lock adapter moves to the insertion position and unlocks the lid of the CentriCult Unit. After running this tool, open the CentriCult Unit manually.

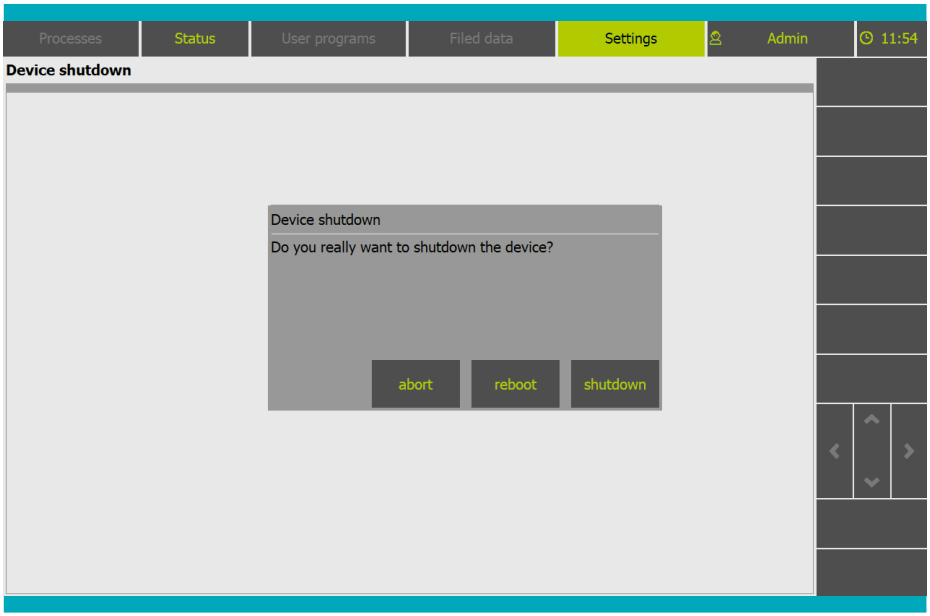
8.2.4 Chamber Out

This tool is used to the CentriCult Unit outside of a running application. The chamber lock adapter moves to the exchange position and unlocks the lid of the CentriCult Unit. After running this tool, open the CentriCult Unit manually.

8.2.5 Shutdown

This tool will shut down or reboot the instrument.

1. Tap <run> in the toolbar to execute the shutdown function.
2. Select abort, shutdown or reboot (see Screen 8.9).



Screen 8.9: Select shutdown or reboot

8.2.6 Recovery

This program enables the rescue of cell products into dedicated bags upon process failure. This tool only supports the following CliniMACS Prodigy Tubing Sets: TS 310, TS 500 and TS 510.

IMPORTANT

Only use this tool under instruction of Miltenyi Biotec Technical Support.

8.2.7 Gas Mix tool

This program enables gas sampling with a sample bag from the gas mix unit.

8.2.8 Instrument Check tool

This tool performs a semi-automated instrument check with some required interaction of the user.

8.2.9 Column Load

In some specific cases, the process allows the enrichment of CD34 positive cells from leukapheresis products.

8.2.10 Custom Files

This program is used to add CAPs to the instrument.

8.2.11 Sealer

This program is used to turn on/off the sealer.

8.3 User settings

The settings can be found in <Settings> ▸ <User settings>.

8.3.1 Set time

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

Note: The time set here will be automatically overwritten if Network Time Synchronization is enabled. To set up Network Time Synchronization see section 9.6 ´Enable network time synchronization´.

8.3.2 Network settings

This setting contains information needed for network integration. For a detailed explanation, refer to the following sections:

- 9.1 for network integration
- 9.2 for LDAP connection
- 9.3 for file sharing
- 9.4 for file transfer via FTP
- 9.6 for network time synchronization

To set up email notification see section 9.5 ´Connecting to an email server´.

8.3.3 Custom settings

Custom settings are general settings for the instrument, including language, company name, department, street, postal code, city, instrument name, contact person, location.

Email notification setting can also be found under customer settings, see section 9.5 ´Connecting to an email server´.

8.3.4 Module settings

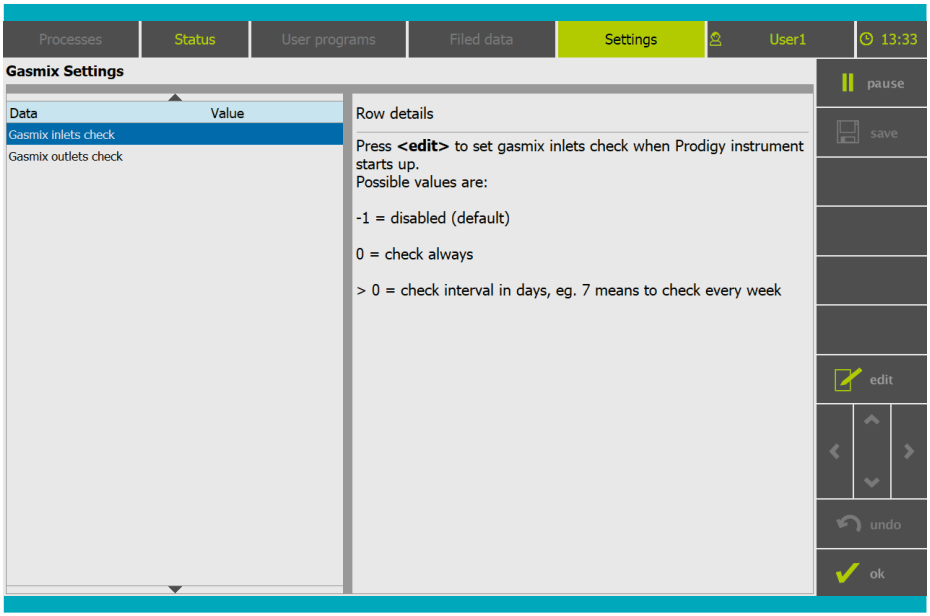
The module settings contain configurations for hardware testing, including:

- Gasmix inlets check
- Gasmix outlets check
- Rotation check
- Supplementary bag reminder

For each of those components, checks can be set to be performed at different time intervals:

- Never (-1)
- Always (0)
- Periodically (enter number in days).

For an exemplary configuration for gasmix inlets see Screen 8.10.



Screen 8.10: Gasmix inlet check

8.3.5 Settings exchange tool

The <Settings Exchange> tool enables copying configurations to multiple instruments. These settings include:

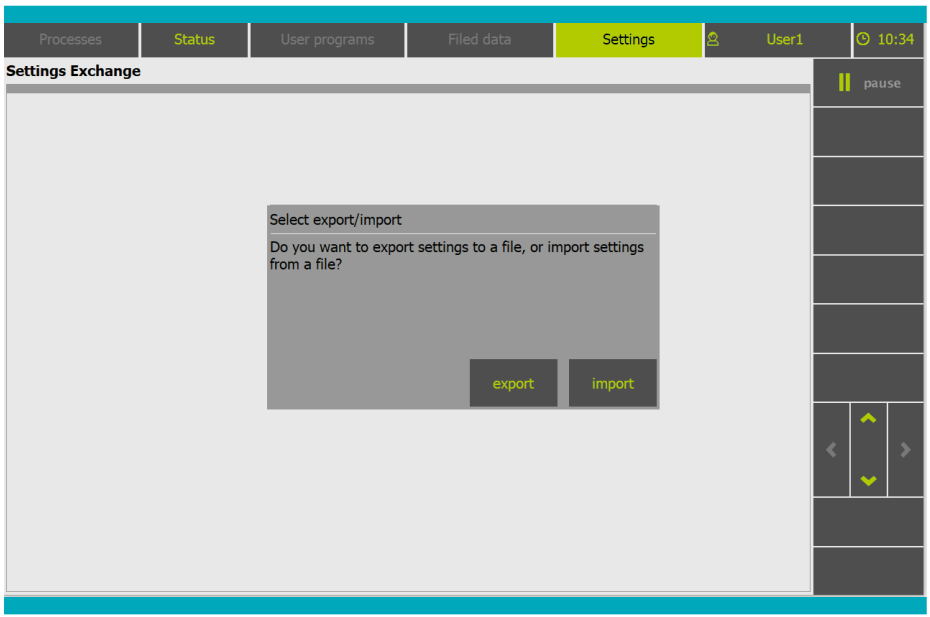
- Customer settings
- Gasmix settings
- Module settings
- Network settings

IMPORTANT

- If using a USB flash drive for importing or exporting, the USB flash drive must be FAT 32 and should not be password protected.
- If file sharing is configured (see section 9.3 ´Connecting to a network drive´) files can also be exported to the file sharing folder.

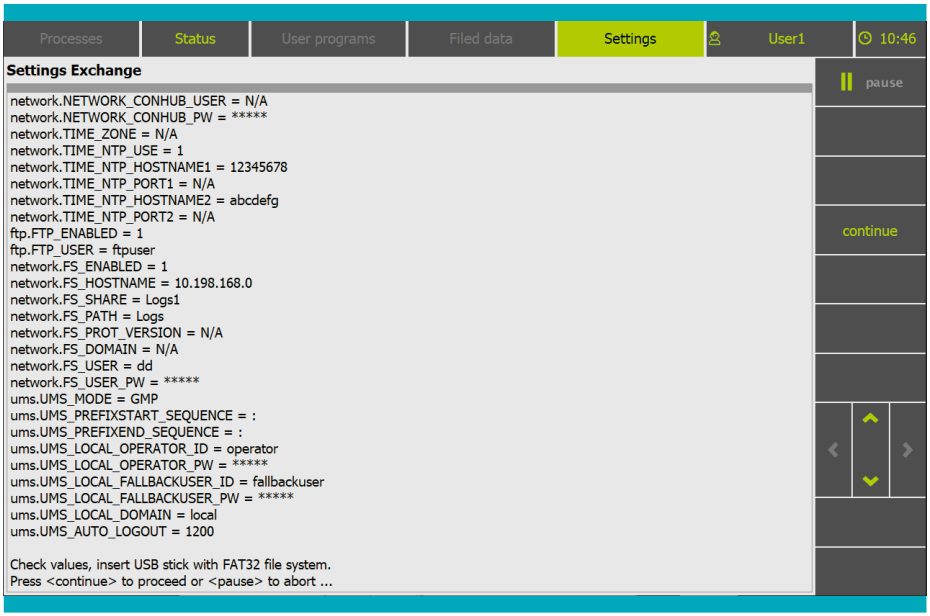
Export settings to USB flash drive

1. Insert a USB flash drive.
2. Go to <Settings> ▸ <User settings> ▸ <Setting Exchange> and tap <run >.
3. Tap <export> on the prompt (see Screen 8.11).



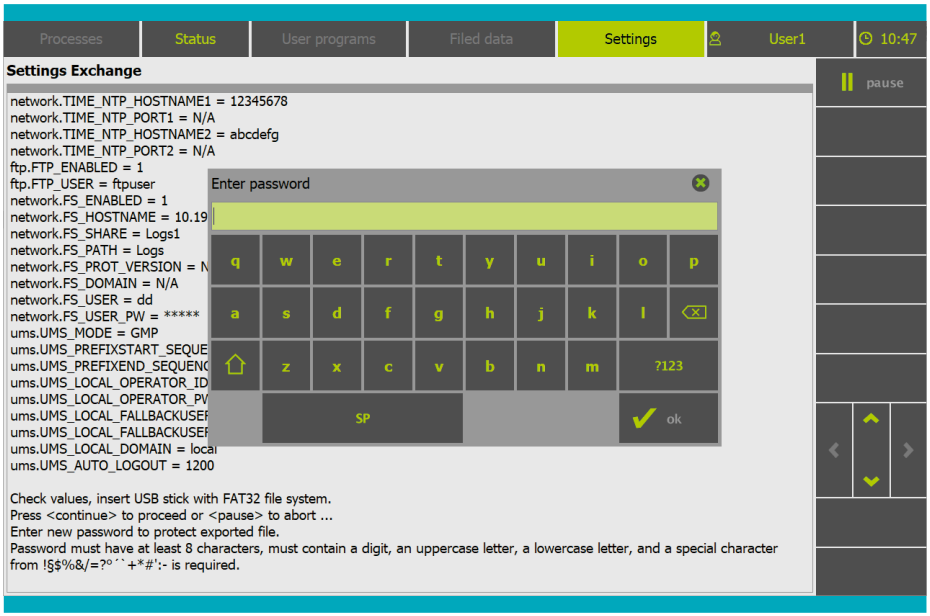
Screen 8.11: Select export

4. Check the values on the screen. Tap <continue> in the toolbar.



Screen 8.12: Check setting values

5. Enter the login password.



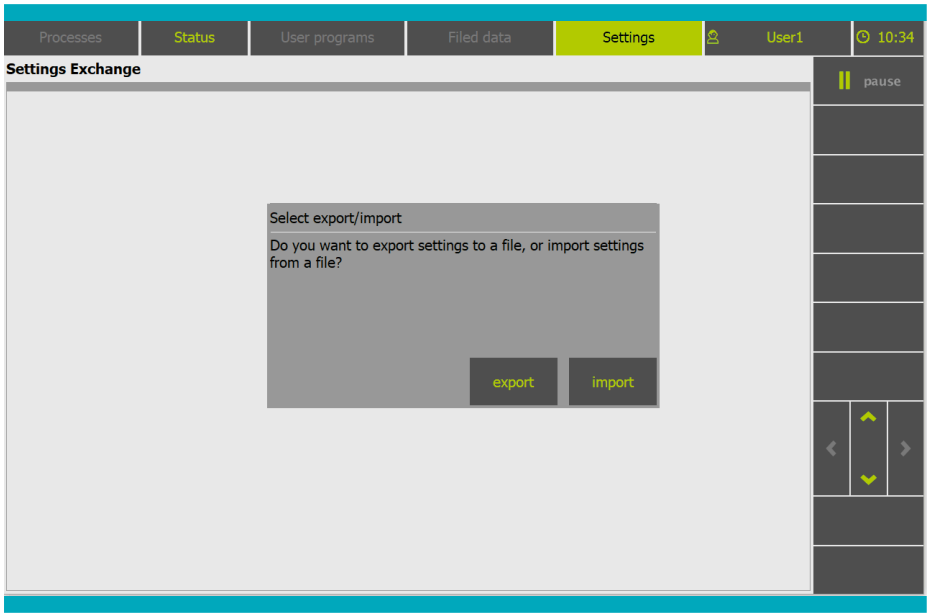
Screen 8.13: Enter password

Import settings from USB flash drive

1. Insert a USB flash drive with the desired user settings file.

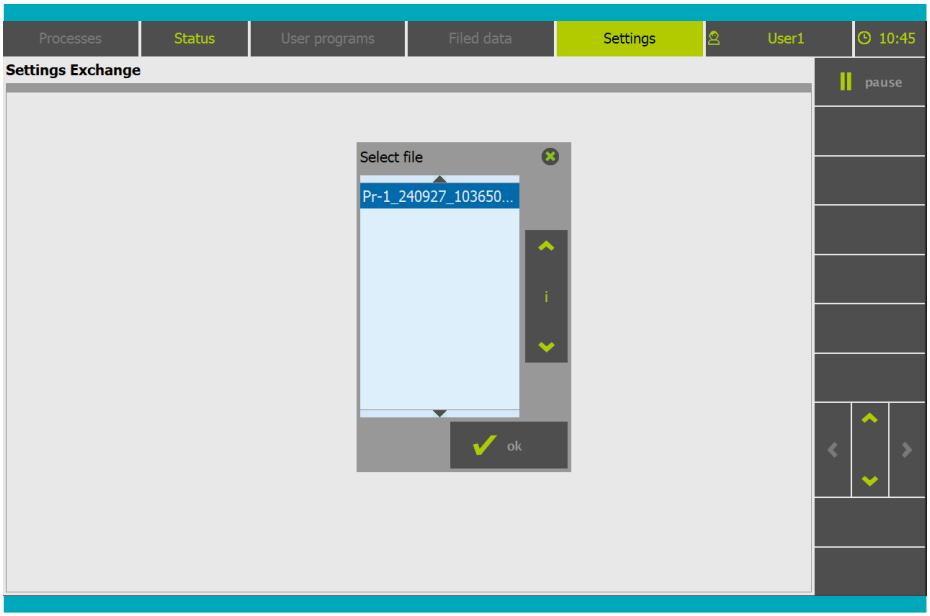
   Note: The USB flash drive must be FAT 32 and should not be password protected.

2. Go to <Settings> ▸ <User settings > ▸ <Setting Exchange> and tap <run>.
3. Select <Import> on the prompt (see Screen 8.14).



Screen 8.14: Select import

4. Select the files to be imported and tap <ok> (see Screen 8.15).



Screen 8.15: Select file to be imported

5. Enter the login password (see Screen 8.13).

8.3.6 SetVolume

This program sets the volume of the speaker on the instrument.

8.3.7 N_2 Settings

This program configures which two out of the three gas ports of the instrument are used (N_2, CO_2, Compressed Air).

9 Network integration

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

- Centralized User Management (LDAP)
- File Transfer via FTP
- Automatic File Sharing
- Email Notification
- Network Time Synchronization

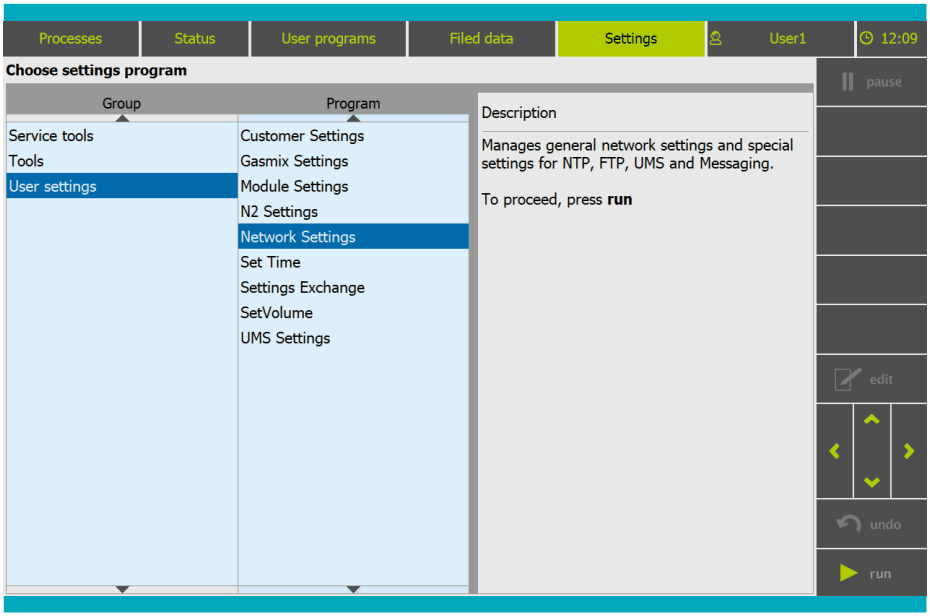
To use the above mentioned functions, first connect the instrument to the local network see section 9.1 ´Connecting to a local network´, then follow the instructions for the specific functions.

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 10 ´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.

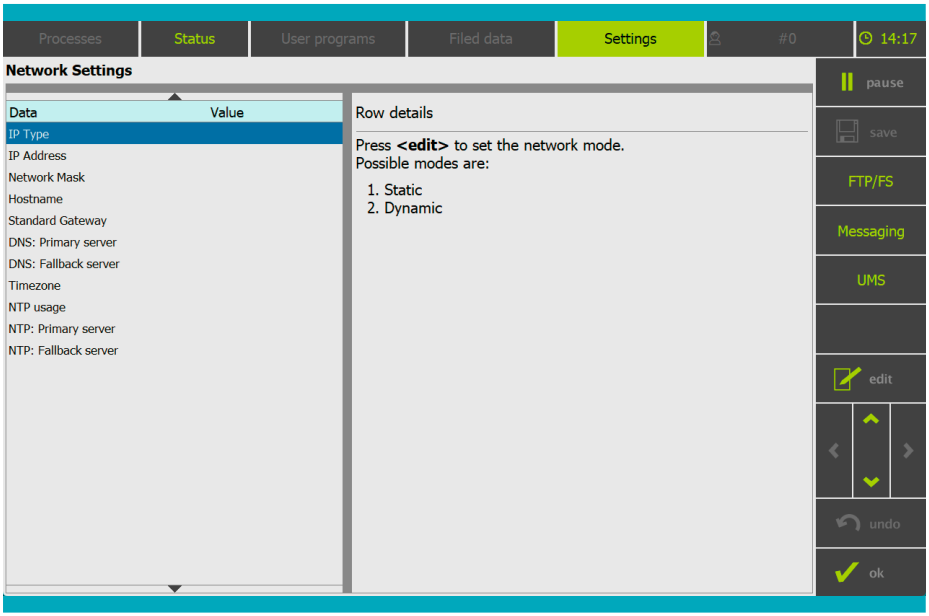
9.1 Connecting to a local network

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> (see Screen 9.1). The Network Settings will be shown (Screen 9.2).



Screen 9.1: Select network settings

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



Screen 9.2: Network settings

For static IP, perform the following steps:

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 Universal Time Coordinated (UTC).
6. Verify that the instrument is connected to the local network.

For dynamic IP, perform the following steps:

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 Universal Time Coordinated (UTC).
4. Verify that the instrument is connected to the local network.

IMPORTANT

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

9.2 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 these steps (see Figure 9.1).

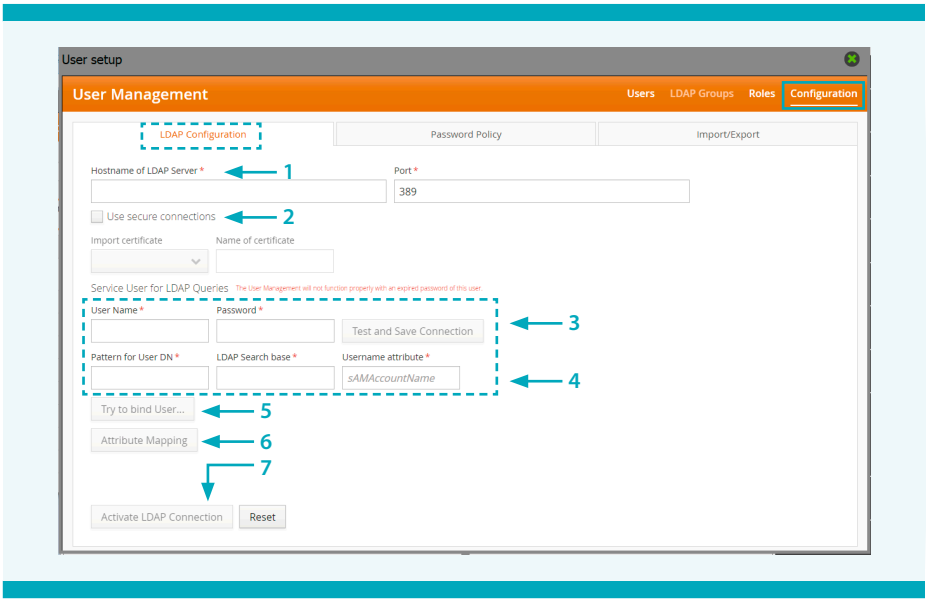


Figure 9.1: User Management menu and the required steps to configure LDAP

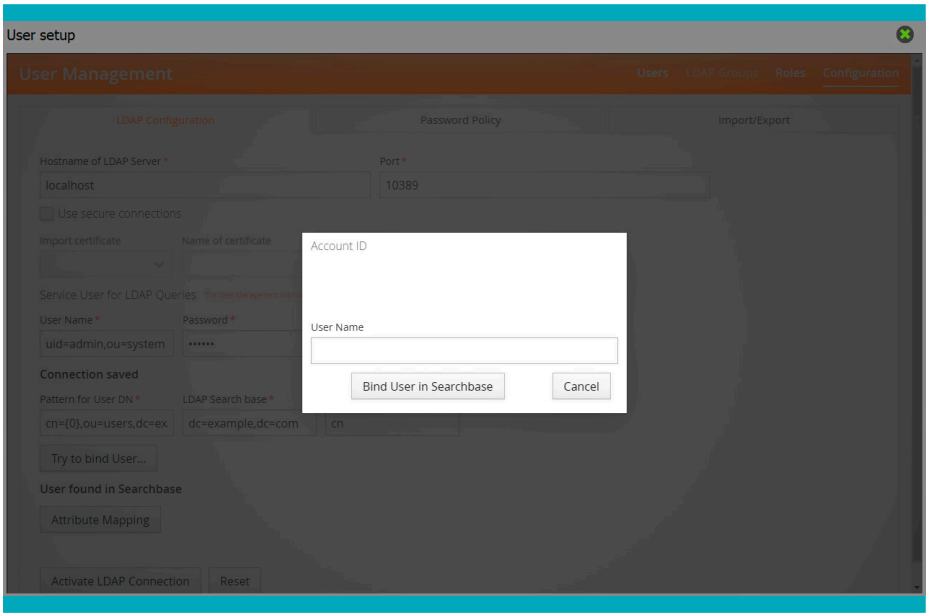
1. Enter the hostname/IP address of the LDAP server.
2. Select a secure connection if required. This will automatically set the port from the standard value 389 to port 636 for a secure LDAP connection. For a secure connection, follow the instruction in section 10.4.2 ´Import UMS settings´ to import certificate in Prodigy Instrument and select the certificate in <import certificate > drop-down list.
3. Enter the username and password of a valid LDAP account. The full LDAP path of the username should be entered. Tap <Test and Save Connection>.
   A pop-up will appear indicating that the connection was successful.

4. 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 something like:

   - Pattern = '<domain>/{0}', for example 'customername_dev/{0}'
   - Search base = 'OU=organization,DC=customername'
   - Username attribute = 'sAMAccountName'

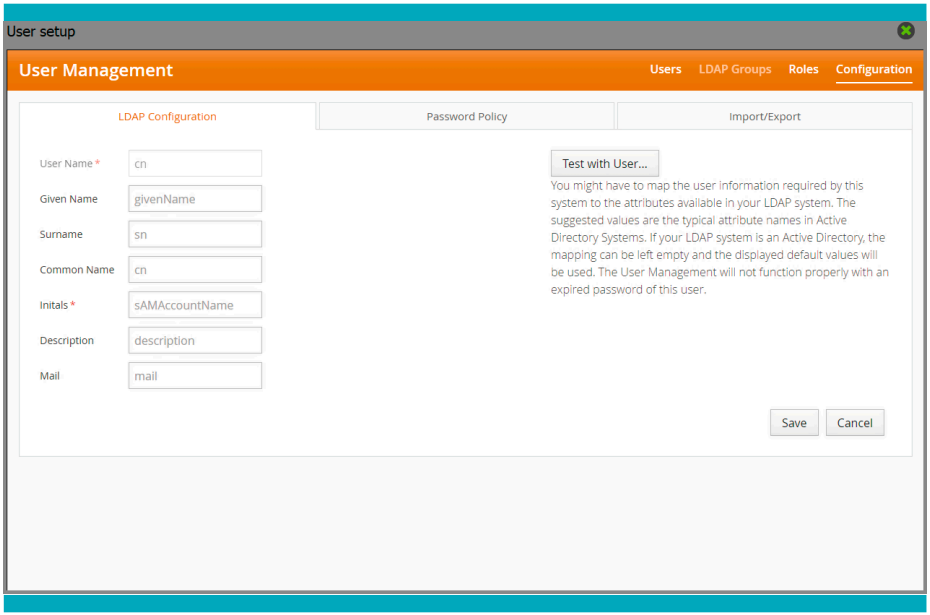
5. Tap <Try to bind User....>. A pop-up will be shown (Screen 9.3). Enter a valid username (the username can be the same username used for the login test). Then tap <Bind User in Searchbase> to continue. If successful, the Account ID pop-up will close; otherwise, an error message will be shown.



Screen 9.3: Account ID input pop-up to enter a valid username

6. Tap <Attribute Mapping>. The attribute mapping will be shown (Screen 9.4). The username attribute entered in step 4 will be automatically mapped to the username. Enter the same value for 'initials' as for 'User Name'. Entering values here will automatically fill out some of the information when a user is created. Tap <save> to return to the LDAP configuration page.

7. Tap <Activate LDAP Connection>. This button will be active if steps 3, 4 and 5 were successful.



Screen 9.4: Example of pre-filled attributes

IMPORTANT

It is necessary to set a value for 'initials' (see Screen 9.4) since this value is considered mandatory information for users of the CliniMACS Prodigy. Missing or improper configuration of the attribute map may cause login failure.

By following these seven steps (see Figure 9.1), the LDAP connection can be fully configured and can now be used to create LDAP groups and LDAP users in the <User Management>. Further details on managing accounts and roles can be found in chapter 10 ´User management´.

9.3 Connecting to a network drive

Automatic file sharing will push all the log files to the network drive after process run immediatly after the application completes. The audit trail records can also be exported to the network drive manually triggered by the user (see section 7.2.2 ´Exporting audit trail´). The automatic file transfer is implemented based on the Server Message Block (SMB) protocol. The supported versions of SMB protocol include SMB 1.0, SMB 2.1, and SMB 3.0 (default).

Note: 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

- SMB server: Make sure this SMB server is reachable. Check the SMB protocol version of this server before starting.
- A pre-created 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).

  Note: Authenticated share is recommended for data security.

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

Setting up the instrument

Note: 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 open FTP/File Share settings, tap <FTP/FS> in the toolbar (Screen 9.2).
2. In < FTP/File Share Settings>, only the parameters in the blue box are relevant for file sharing (see Figure 9.2).

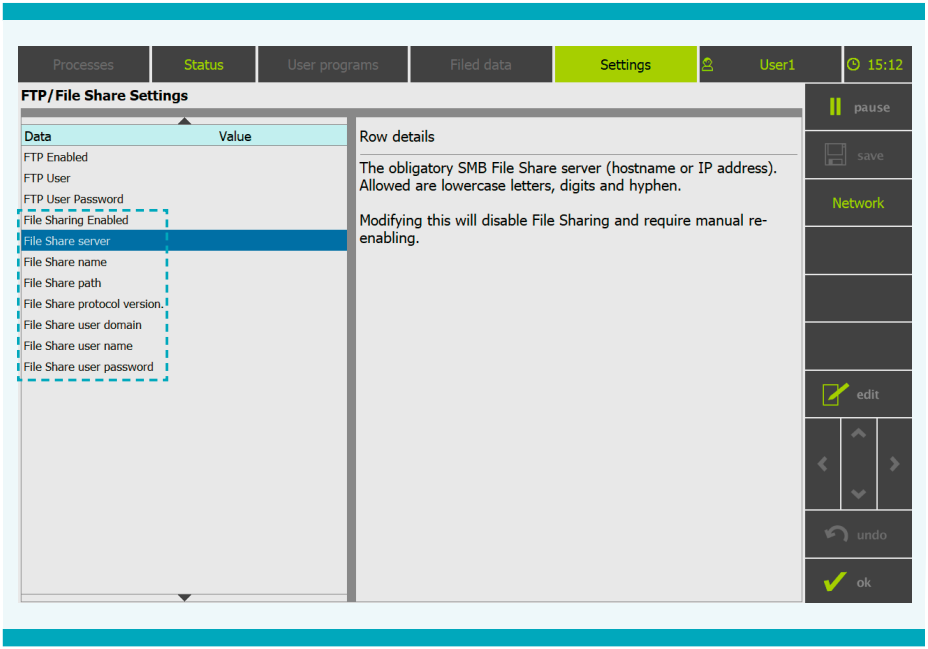


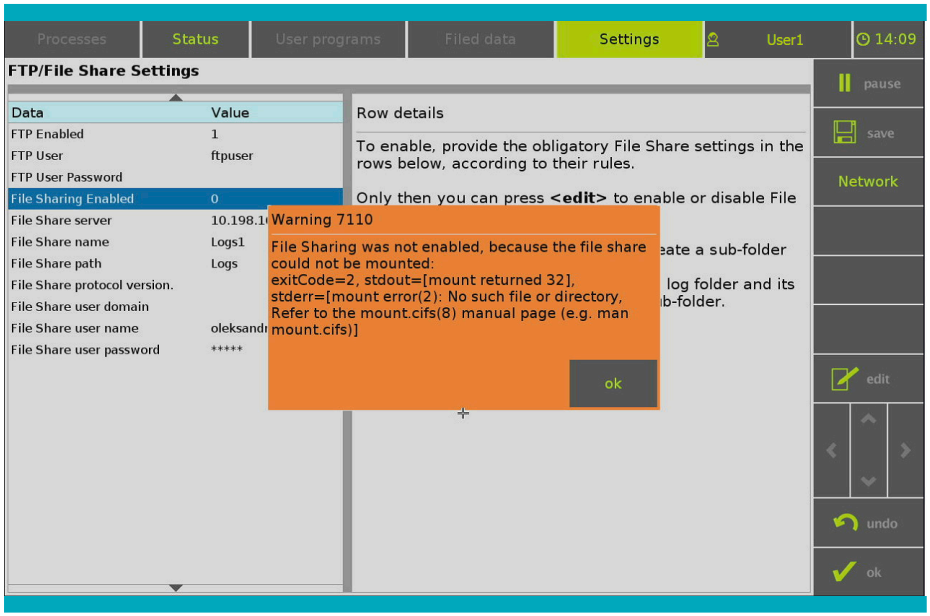
Figure 9.2: Parameters for file sharing

2. To enter the hostname or IP address of the SMB server, select <File Share server> and tap <edit>.
3. To enter the Share Name, select <File Share name> and tap <edit>.
4. (Optional) select <File Share path> and tap <edit> to enter the path.
   If this path is entered, the instrument-generated files will be pushed to \\[File Share server]\[File Share name]\[File Share path]\

   If this path is empty, the generated files will be pushed to \\[File Share server]\[File Share name]\
   If the folder is not found, the software will give a warning (Screen 9.5).

IMPORTANT

It is recommended not to use spaces in File Share path.



Screen 9.5: Warning for file sharing setup failure

5. To enter the SMB protocol version select <File Share protocol version> and tap <edit>.

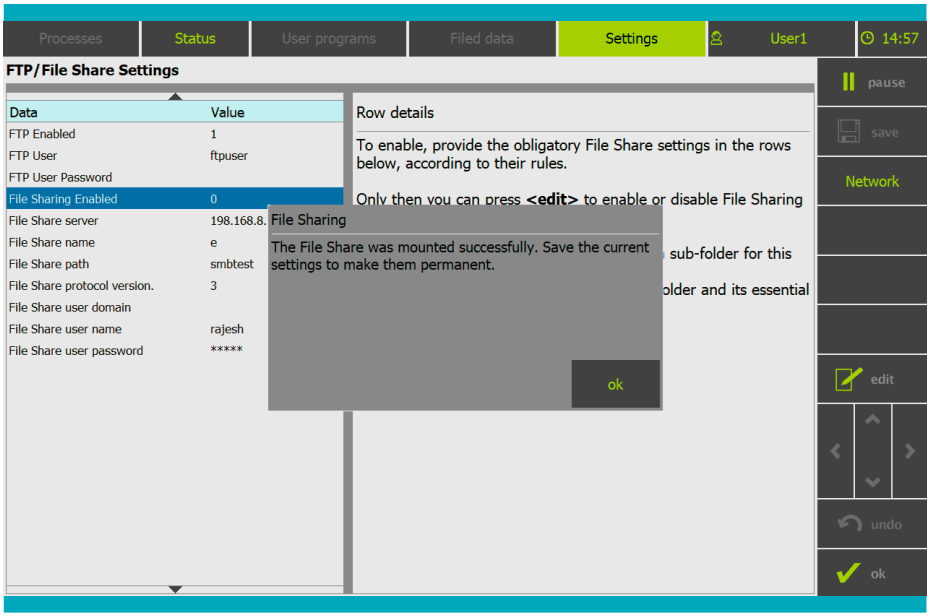
6. To enter the user domain select <File Share user domain> and tap <edit>. Repeat the steps for <File Share user name> and <File Share user password>.

IMPORTANT

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

7. Set <File Sharing Enabled> to 1.

After configuration, a popup will show the success of configuration (see Screen 9.6).



Screen 9.6: Successful setup for file sharing

IMPORTANT

Modification of file sharing parameters will disable file sharing and it needs to be re-enabled manually. Always confirm that 'File Sharing Enabled" is enabled (value set to 1).

9.4 Configure file transfer via FTP

FTP is a network protocol that allows the transfer of data between the CliniMACS Prodigy (referred to as FTP server) and the end user's computer (referred to as FTP client) over IP (Internet Protocol) connections.

IMPORTANT

- Ensure that the FTP connection is used only in an internal network, without access to and from the internet. The security of the network must be ensured by the user.
- Ensure that the firewall settings on the client computer are configured appropriately for FTP active or passive connections to allow data exchange with the instrument.

Note: Data accessible from the CliniMACS Prodigy over FTP is read-only and can only be downloaded

To connect the FTP client to the instrument, login is required. The instrument needs to be configured differently according to the login option. Two login options are supported:

- Login option 1: A registered account in UMS. Make sure 'File management user' role is assigned to this account. In this case, the connection establishment and termination will be recorded in the audit trail. For more information regarding roles and user management, see chapter 10 'User management'.
- Login option 2: A local username and password saved in FTP/File Share Settings.

9.4.1 Setting the instrument

1. Go to <FTP/File Share Settings>. Only the parameters in the blue box are relevant for FTP.

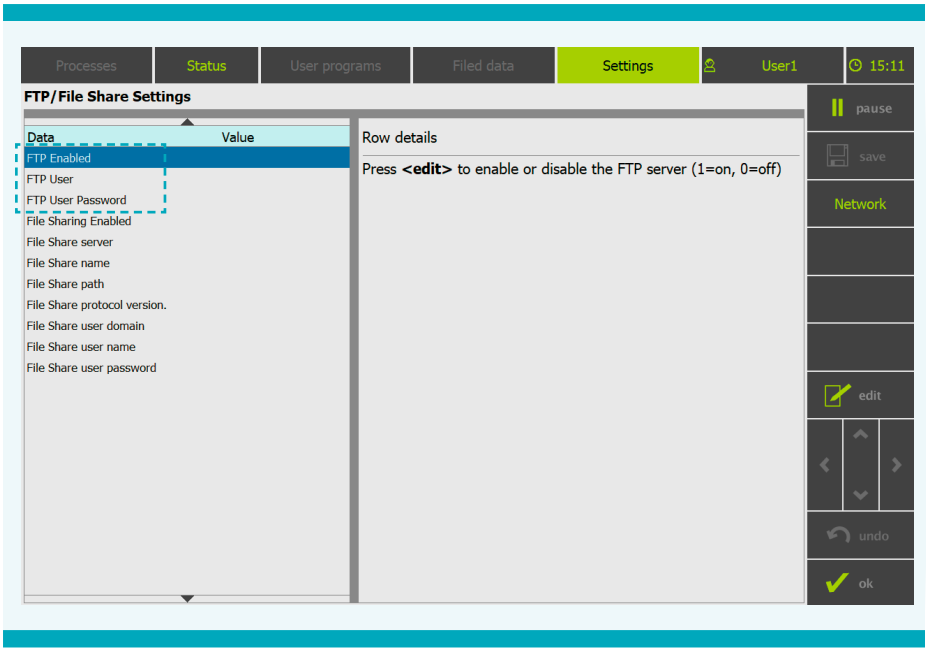


Figure 9.3: Parameters for file sharing

2. (Skip this step, for login option 1) to enter the username when login from the FTP client, go to <FTP User> and tap <edit>. The username used for the FTP client does not need to be registered in the user management system. The username must begin with a letter and may contain lower and upper case characters, numbers and underscores.

   Note: If <FTP User> is set to 'N/A', the FTP connection will be disabled.

3. (Skip this step for login option 1) To enter the password, go to <FTP User Password> and tap <edit> . The password must contain at least six characters and may consist of lower and upper case characters, numbers as well as the special characters ,.:+#!?=.
4. To enable the FTP connection, go to <FTP Enabled> and set value to 1 by entering in the input field.
5. To save the settings tap <ok> on the toolbar.

9.4.2 Connecting with FTP client

The user can connect to the instrument with any available FTP client (e.g., FileZilla) to download protocols and log files after setup. To connect to the instrument, enter the following information:

- The IP address of the instrument. It can be found under <Settings> ▸ <Tools> ▸ <Info> ▸ <Network information>.
- The port: use standard port 21.
- Username and password:
  For login option 1: Enter the account ID and password registered in the user management.
  For login option 2: Enter the username and password setup as previously described in step 2 and step 3.

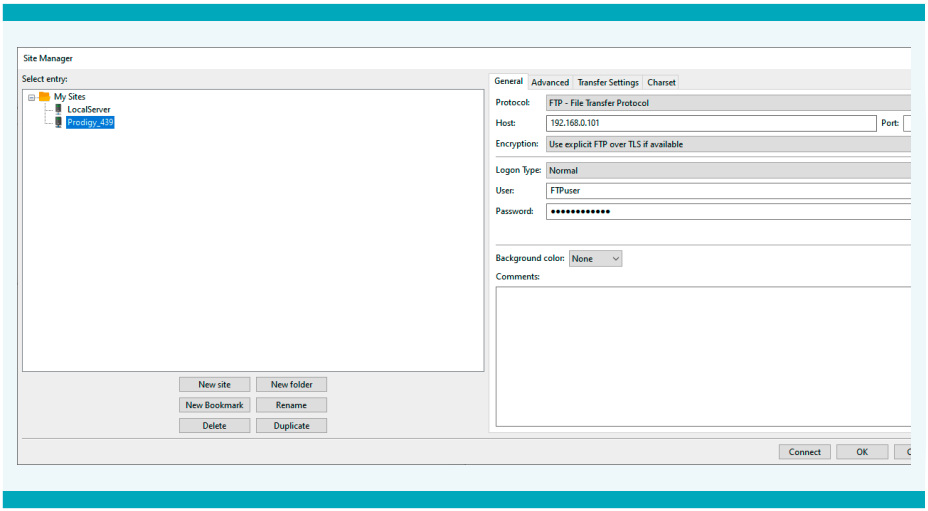


Figure 9.4: Exemplary connection parameters

Note: An individual user may only establish a single connection at a time, as multiple connections are not allowed by the instrument's server. If a client software is used that uses simultaneous connections (e.g., FileZilla) change the settings of the client accordingly to allow only a single session. Otherwise, the contents can only be browsed but not downloaded.

9.5 Connecting to an email server

The software can send out an email to a pre-entered email address in case of error and/or warning messages during a process run. The email will contain warning/ error messages and a screenshot of the instrument (see Figure 9.5). The email notification supports Simple Mail Transfer Protocol (SMTP) and Simple Mail Transfer Protocol Secure (SMTPS).

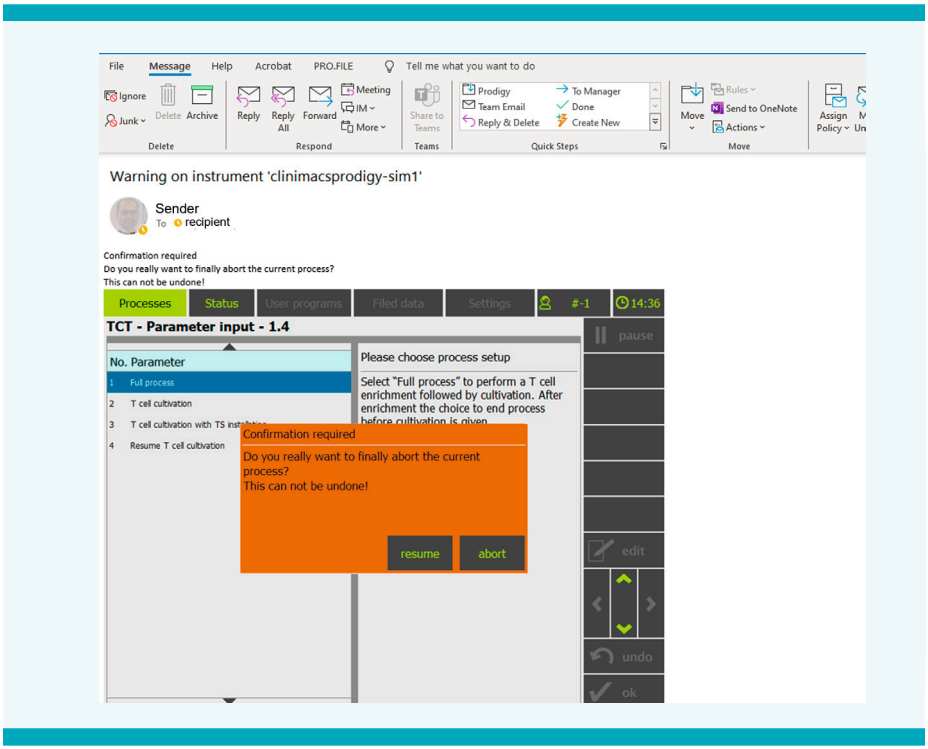


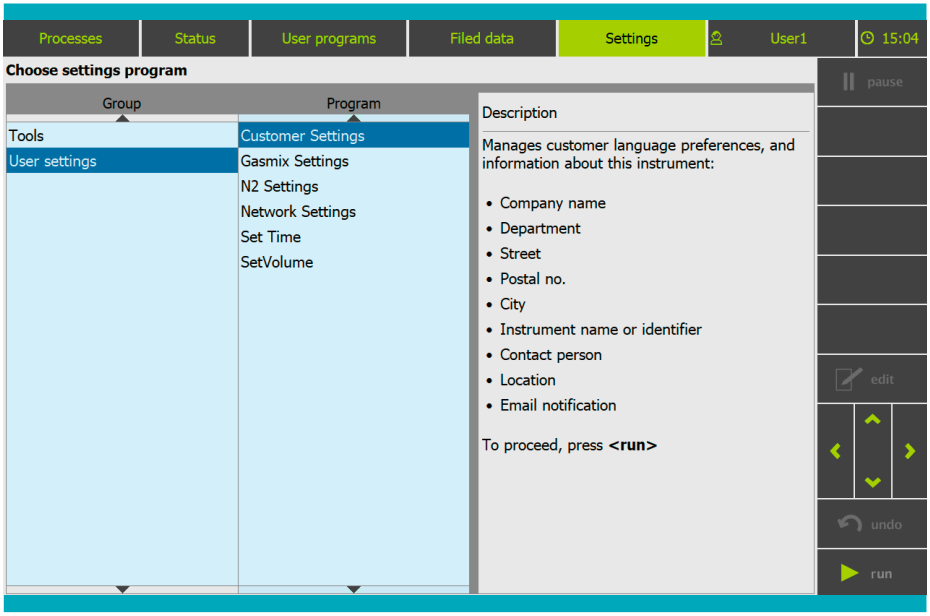
Figure 9.5: Example email

Prerequisites:

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

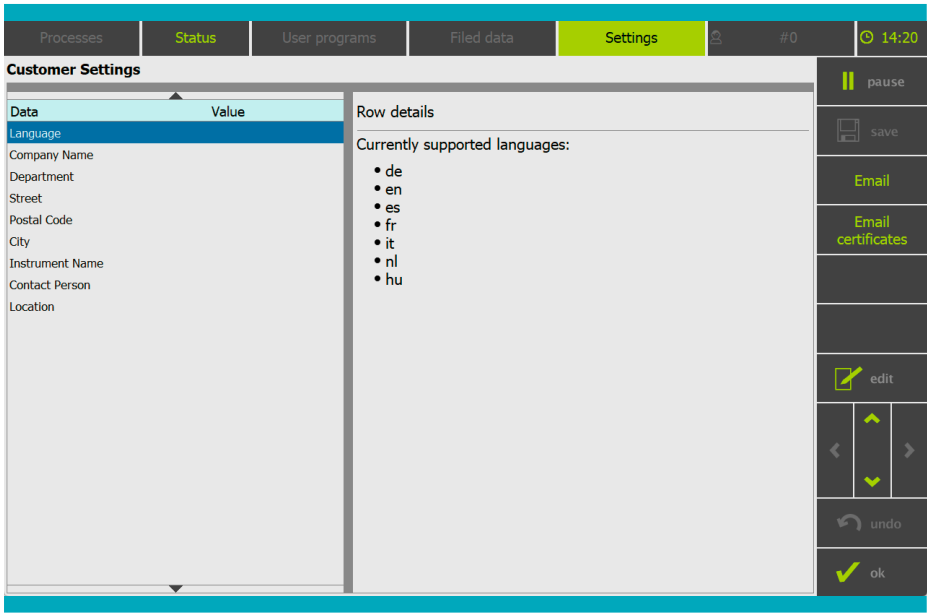
Setting up the instrument:

1. To enter customer settings, go to <Settings> ▸ <User settings> ▸ <Customer Settings> and tap <run> (see Screen 9.7).



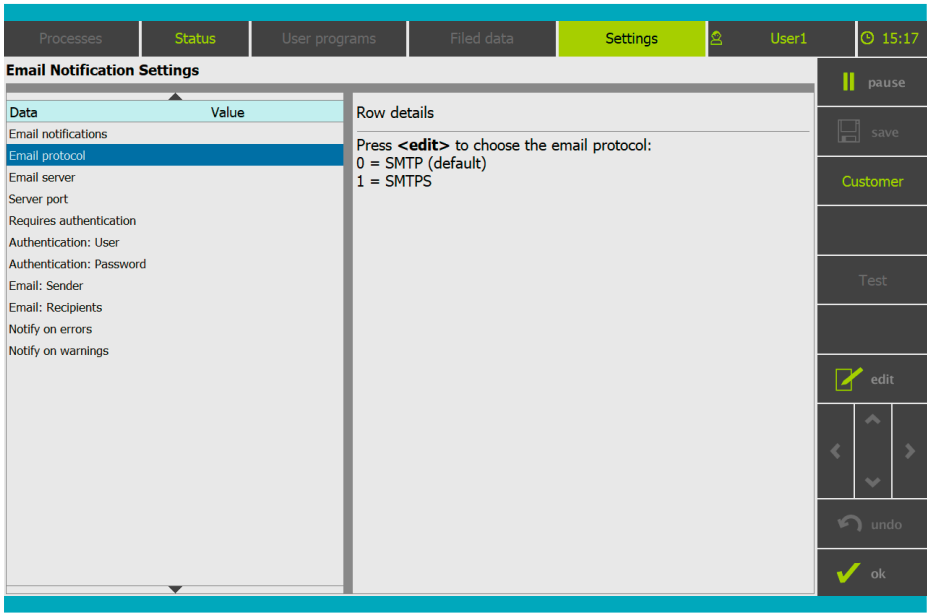
Screen 9.7: Start customer settings

2. To enter <Email Notification Settings> tap <Email> in the toolbar (see Screen 9.8).



Screen 9.8: Email settings

3. To enter the value corresponding to the protocol used by the email server, go to **<Email protocol>** and tap **<edit>**. By default SMTP(0) is selected.



Screen 9.9: Parameters for email notification

4. To enter the hostname or IP address of the email server, go to **< Email server>**.

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

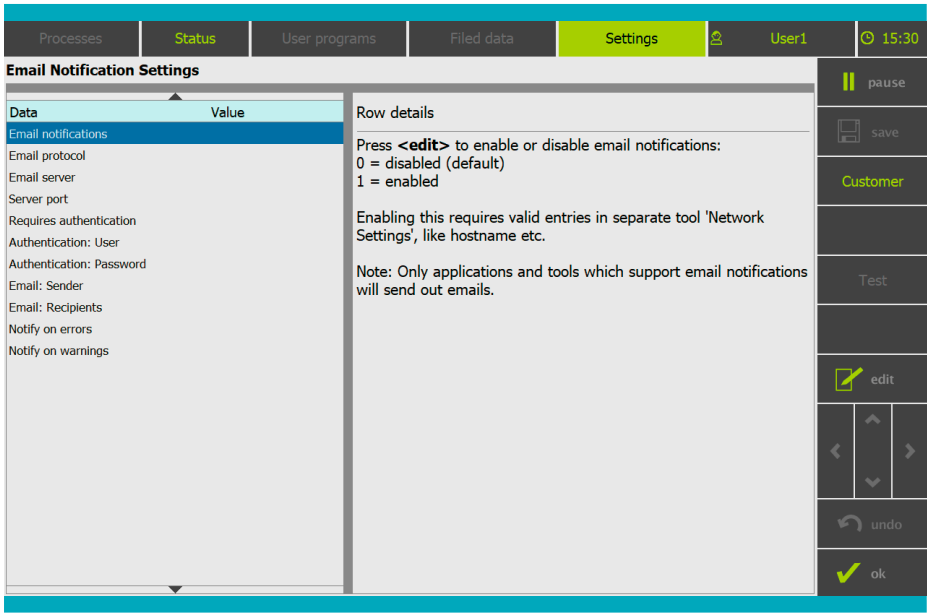
If the standard port is used, there is no need to edit this field.

Protocol	Default port	Alternative port
SMTP	25	2525, 465, 587
SMTPS	465	587 (TLS)

Table 9.1: Port for email server

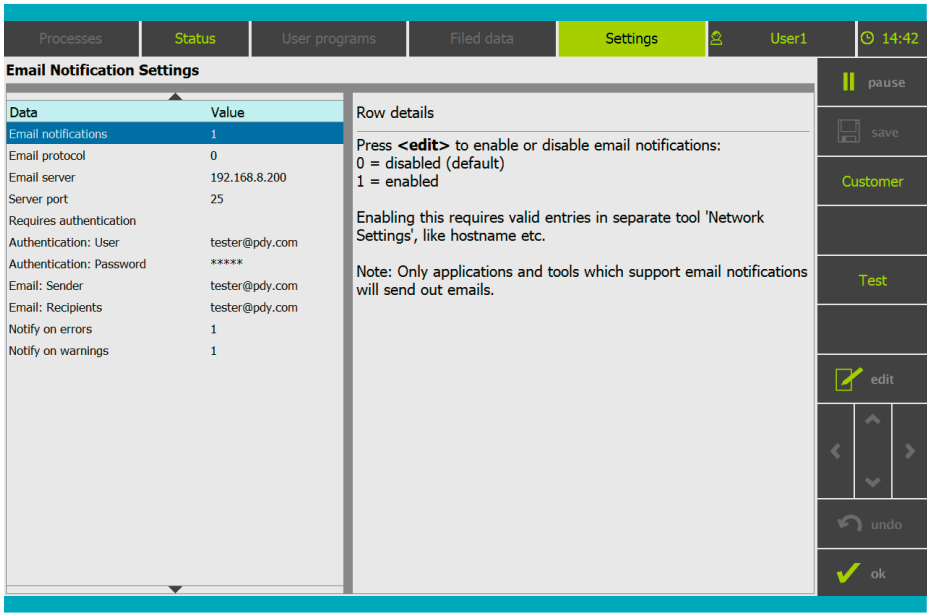
6. Select <Requires authentication>. If the email server requests authentication, set this field to 1, and enter authentication username and password as described in step 7, otherwise go to step 9.
7. To enter the username and password, go to <Authentication: User > and <Authentication: Password>.
   Note: Multiple instruments can share one authentication account. Consult your IT department for assistance if required.
8. 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.
9. To enter the email addresses of the recipients, go to <Email: Recipients> and tap <edit >. The recipients can also be a group email address.

   Note: Multiple recipients may be entered, separated by a space.
10. 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).
11. 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).
12. To enable email notifications, go to < Email notifications> and tap <edit> (see Screen 9.10). Set to 1 to enable notifications. By default, email notifications are disabled (value set to 0).



Screen 9.10: Enable email notification

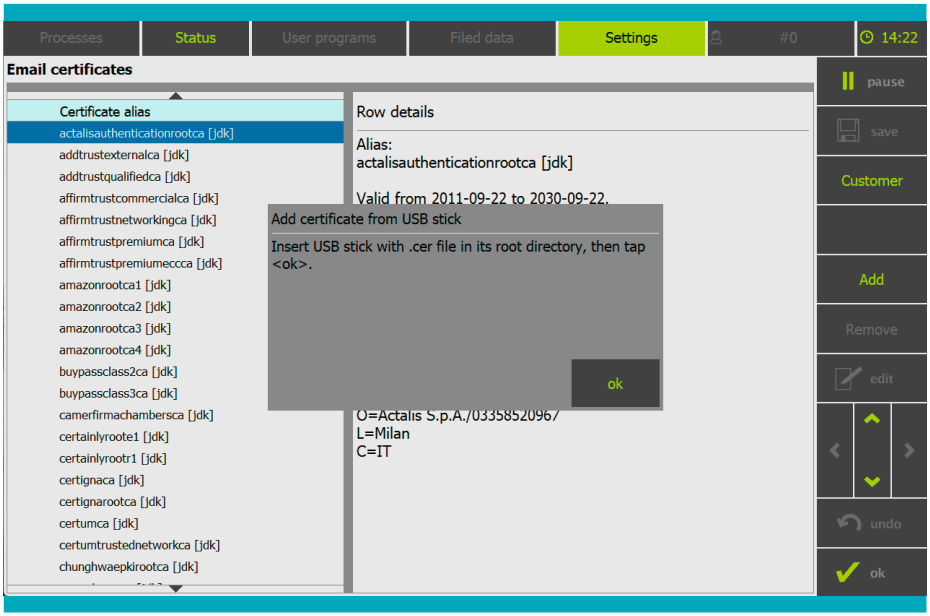
13. After all required information is entered, <Test> button in the tool bar is enabled. To send a test email, tap <Test> in the toolbar.



Screen 9.11: Send test email

Email certificates

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



Screen 9.12: Add certificate from USB stick

To add a new certificate, tap <Add> and follow the instructions on the screen.

9.6 Enable network time synchronization

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>. The network configuration appears. Parameters in blue box are relevant for network time synchronization (see Figure 9.6).

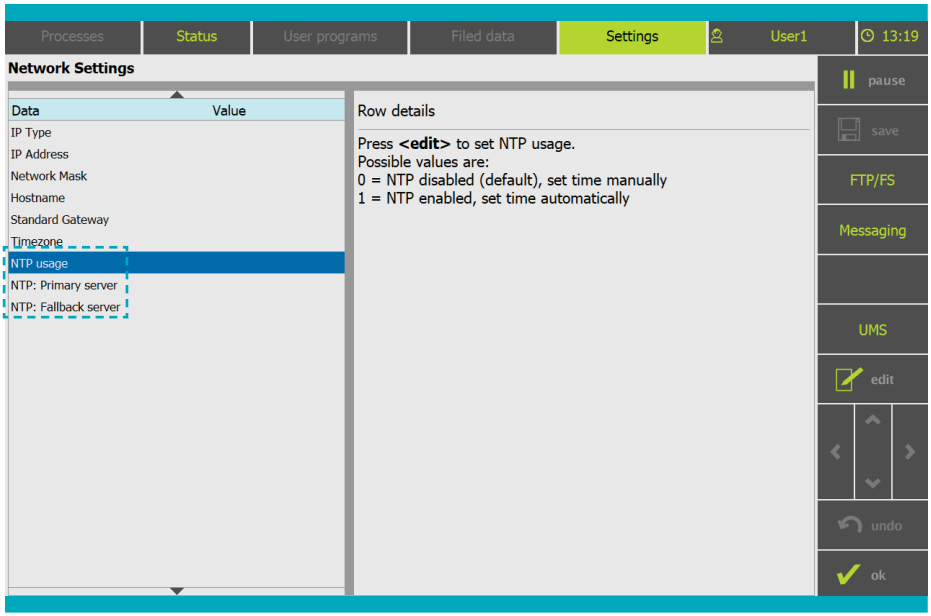


Figure 9.6: NTP setting

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 8.7 ´Shutdown´).

10
User management

10.1 General information

The user management system in the software 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.

Rights

Rights represent the minimum assignable unit of user actions. The rights are defined by the software and the user can only group the existing rights. For an overview of the different rights in the software, see Table A.1 in the Appendix.

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. Important default roles are listed in Table 10.1. The software supports customized roles.

Accounts

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

Role	Tools/Rights
Application x.x operator	Permission to run this application with version number x.x
ATS user	Access to Audit Trail including viewing, exporting and deleting
Administration tools user	Access to tools for administrating the instrument. Suggested for administrators
Common tools user	Access to common tools: info, license, shutdown, and user settings. Suggested for all users
File management user	Access to Backup Filed Data tool and Custom Files tool. Enable log file access via FTP
Gas mix tool v1.0 Operator	Access to the gas mix tool
Injected programs	Permission to run injected programs
N_2 settings tools user	Access N_2 settings tool
Set time user	Allows to set the time
Support tools user	Chamber in, chamber out, sealer, and instrument check
UM Administrator	Access to the User Management allowing to manage accounts
UM user	Defined operator who shall start and run user applications

Table 10.1: Overview of default roles

In the following is an example of a conventional UMS setup:

- 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.
- An operator starts and runs applications on the instrument. The operator account would be set up to allow running a particular set of applications and tools based on customer user management decisions to support and troubleshoot. There can be more than one customer defined user type and each user can be assigned one or more roles.

IMPORTANT

For an operator, the role 'UM User' must be assigned. For an administrator, the role 'UM Administrator' must be assigned.

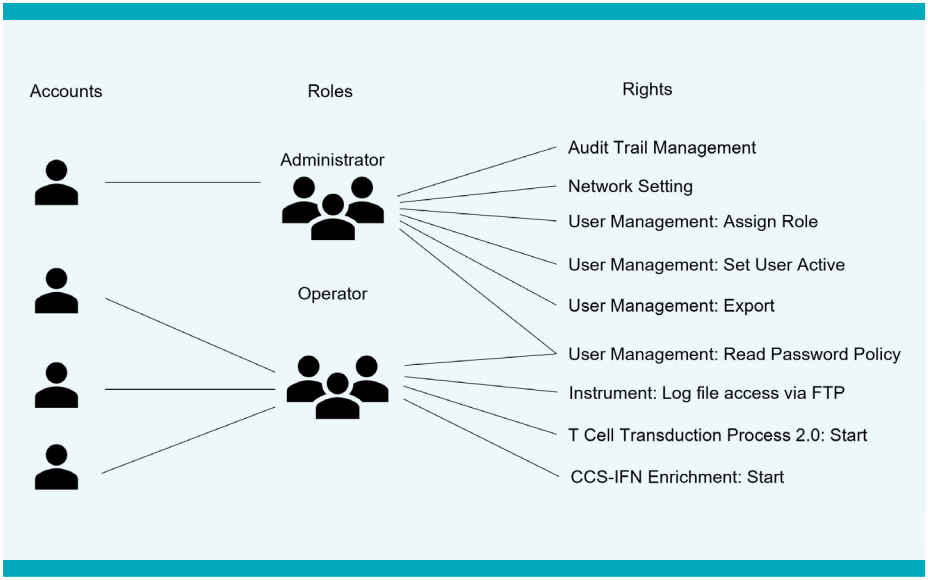


Figure 10.1: Exemplary connection parameters

⚠ CAUTION

Risk of process failure due to failed login. If login is not possible anymore, there is the risk of process failure. To avoid such a situation, appropriate user and administrator accounts with distinct passwords need to be created before initiating the start of an application on the instrument. In case an instrument login is not possible anymore, contact Miltenyi Biotec Technical Support.

IMPORTANT

- 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 and all users and administrators need to be trained accordingly.
- If the LDAP connection fails, use a local user account to access the instrument.

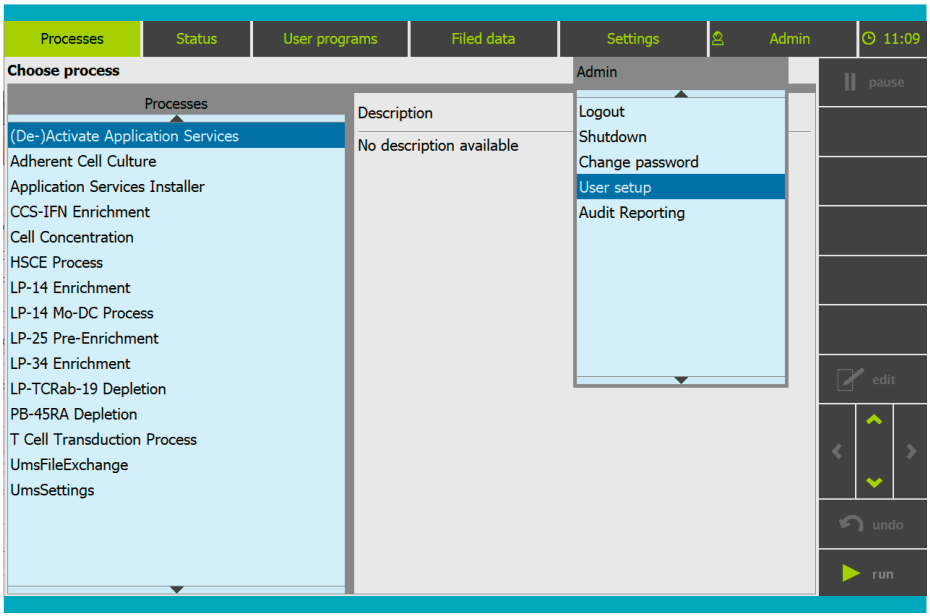
10.2 Manage roles and accounts

IMPORTANT

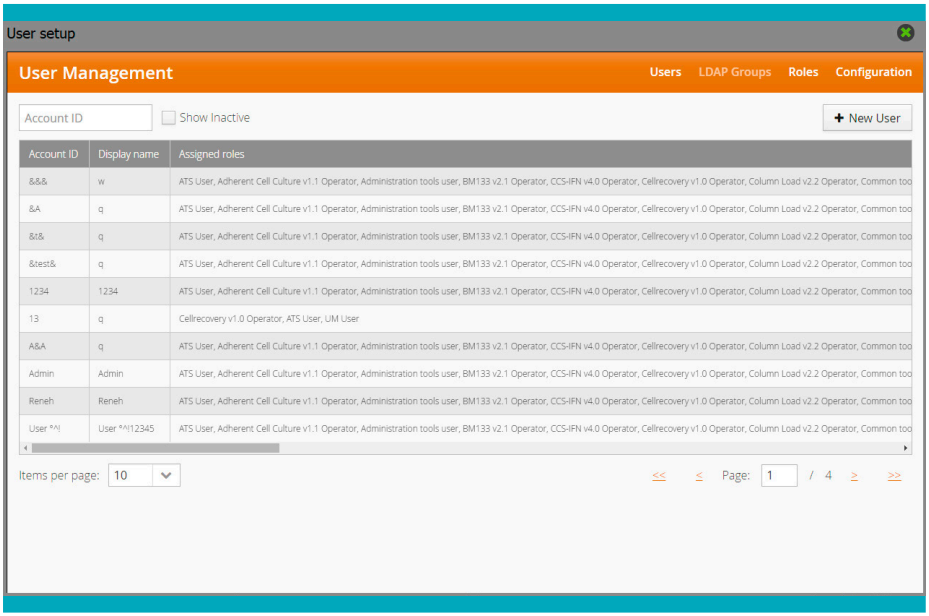
A user must have the role 'UM Administrator' to configure user management system.

10.2.1 Access to user management

To enter the User Management System go to (quick access menu) and tap <User setup>. The user management page will be shown (Screen 10.2). The user management has four pages: <Users>, <LDAP Groups>, < Roles>, and <Configuration>. By default, <Users> is selected.



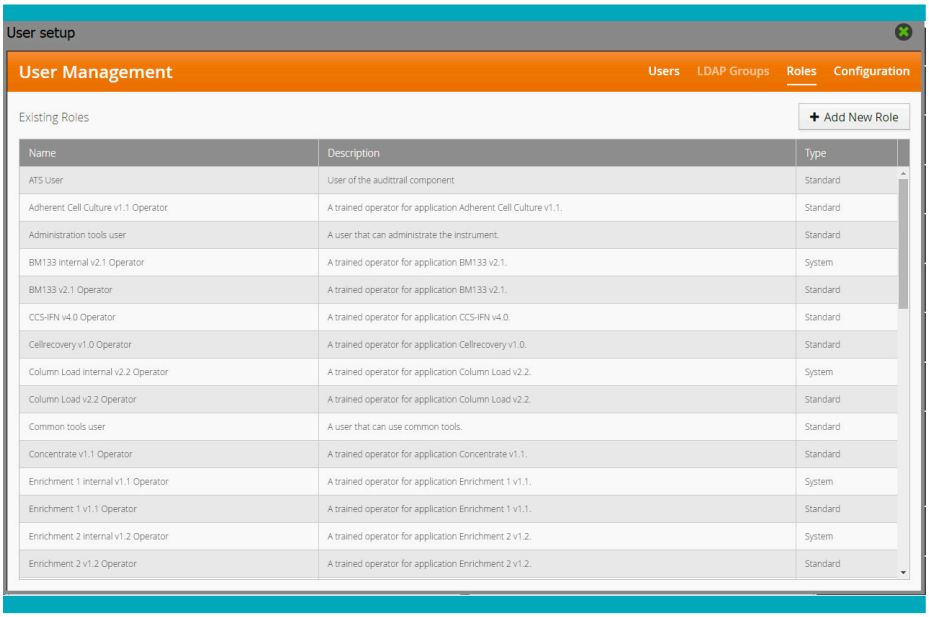
Screen 10.1: Select User setup



Screen 10.2: User Management menu

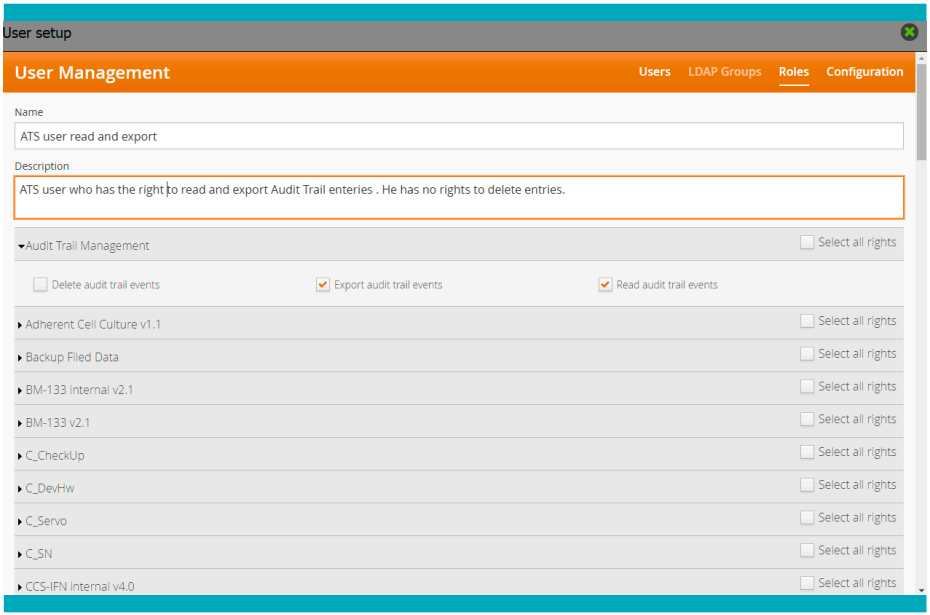
10.2.2 Create a new role

1. Tap <Roles> in the <User Management>. A list of existing roles is shown (Screen 10.3).



Screen 10.3: Defined roles in user management

2. Tap <+Add New Role> (Screen 10.3). A new role definition page will be shown (see Screen 10.4).



Screen 10.4: Create a new role

3. Enter the name and description of the role. Tick the desired right for this role.
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.

10.2.3 Change rights of roles

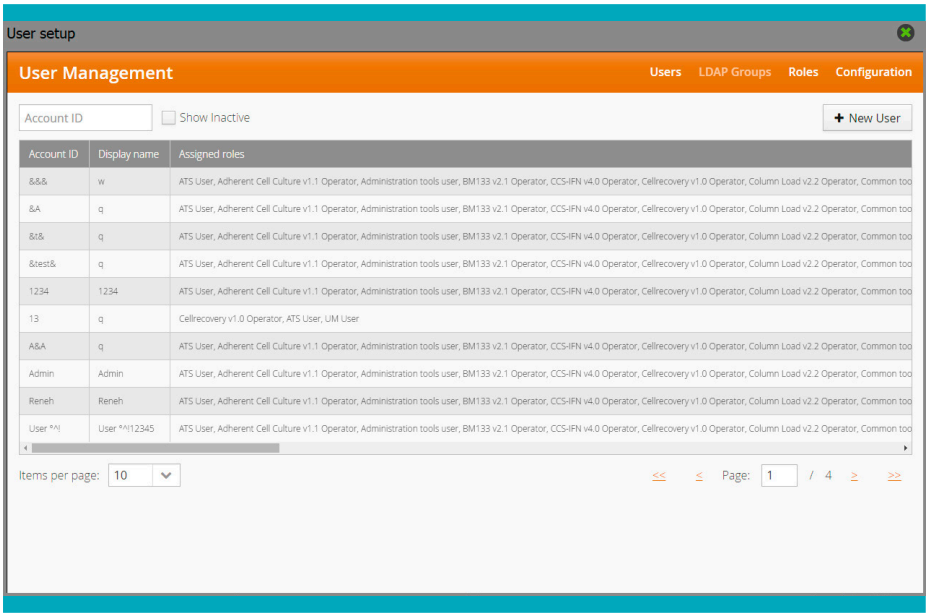
1. Find and select the role in the list of existing roles (see Screen 10.3)
2. Select or deselect the desired rights.
3. Scroll down to the bottom and tap <save>.

10.2.4 Add a local user

IMPORTANT

- A user must have the role 'UM Administrator' to create a new account.
- In a GMP environment, real names or synonyms that can be clearly distinguished and recognized must be used.

1. Select <Users> menu in the user management.
2. Tap <+New User>. A new user page will be shown (Screen 10.5).

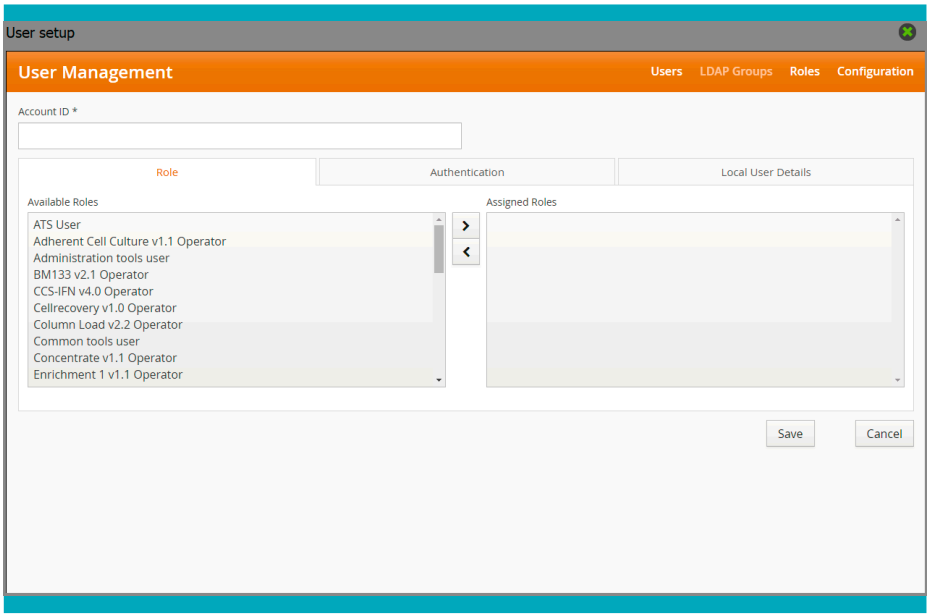


Screen 10.5: New user menu

3. Enter account ID (Screen 10.6). 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.

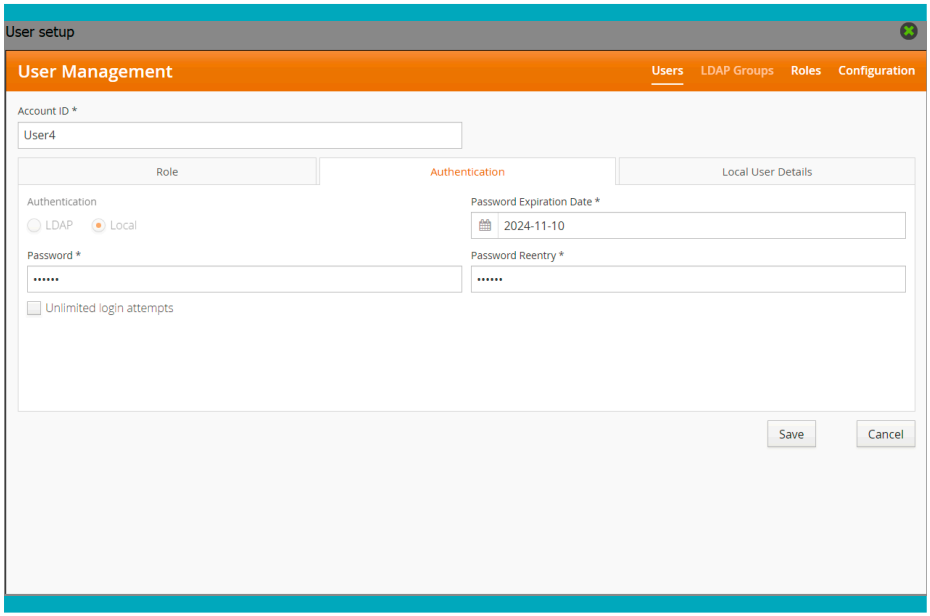
   If Active Directory is configured, the software will check if this ID is registered in AD server. If the ID is not found, a local account will be created. If the ID is found, the AD account will be used by default. To change an LDAP account to a local account, follow step 5.

4. To assign the corresponding roles to this account, select the entry in <Available Roles> in the <Role> tab, and tap ⊡ (Screen 10.6). To remove an assigned role of this account, select the entry in <Assigned Roles> and tap ⊡.



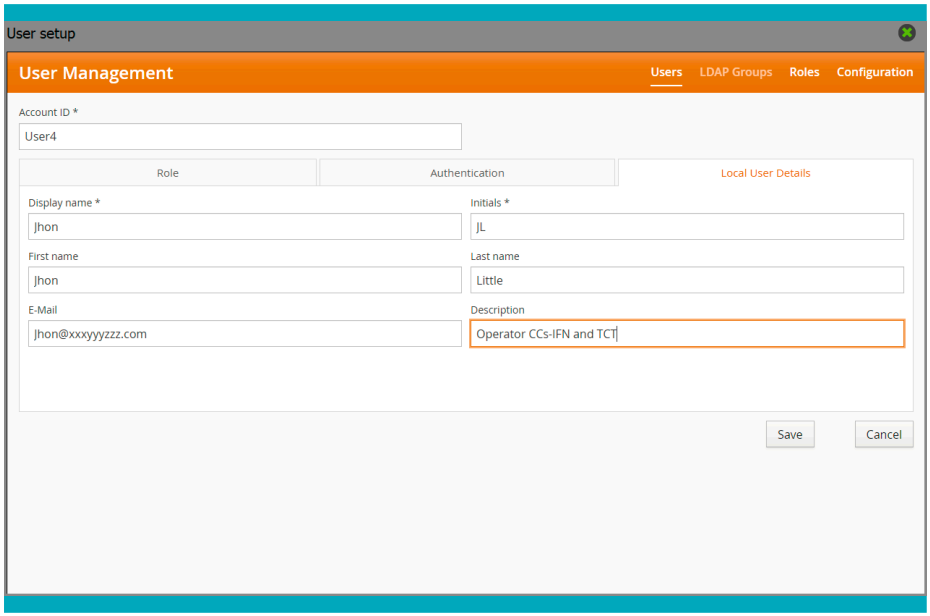
Screen 10.6: User configuration page

5. 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. For a local user, enter the password and set the expiration date, following the password policy (see section 10.3 ´Configure password policy´).



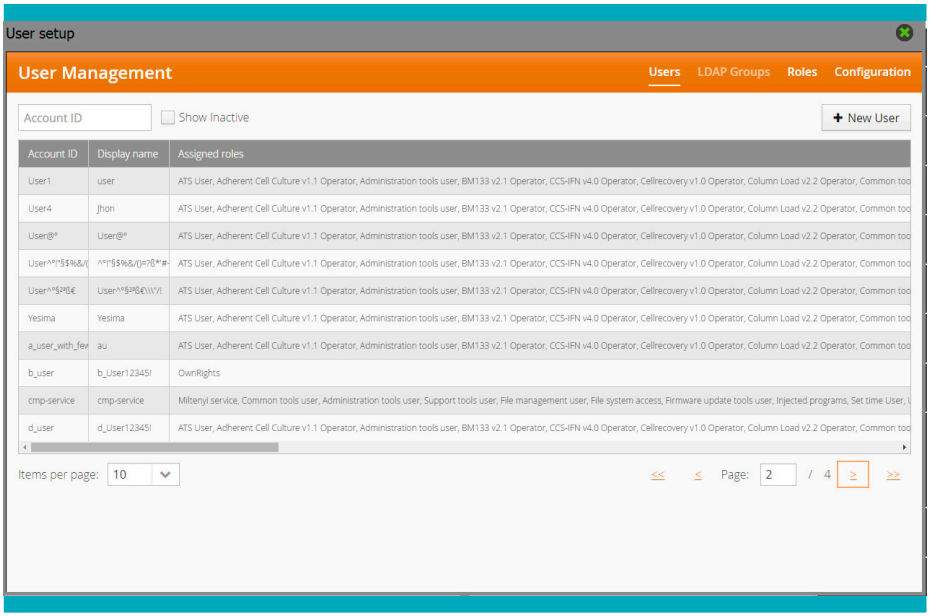
Screen 10.7: Enter password of new user

6. In the <Local User Details> tab, set more detailed information of this account.



Screen 10.8: Enter details for local user

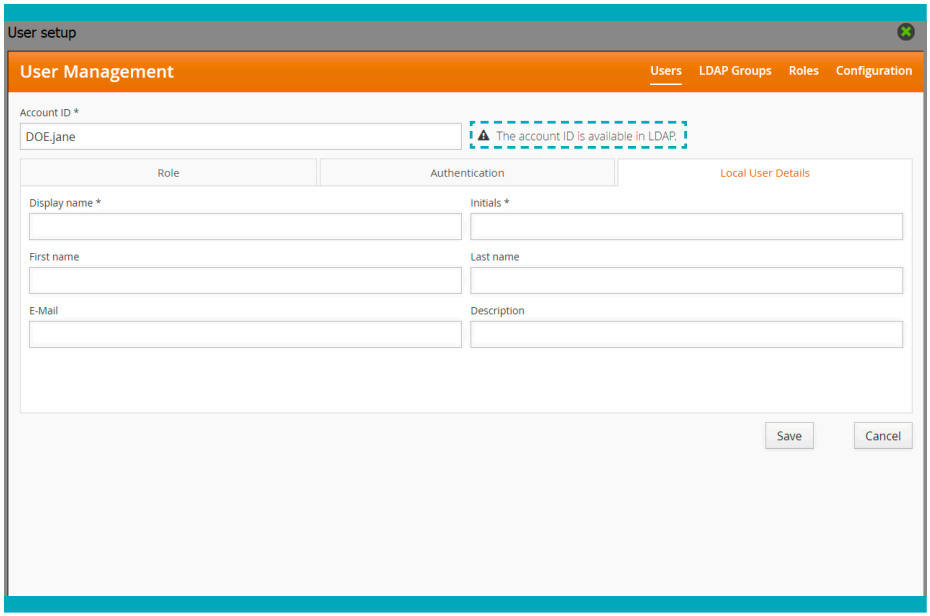
7. Tap <save>. The new added account is shown in the account list (Screen 10.9).



Screen 10.9: Confirmation of new added user

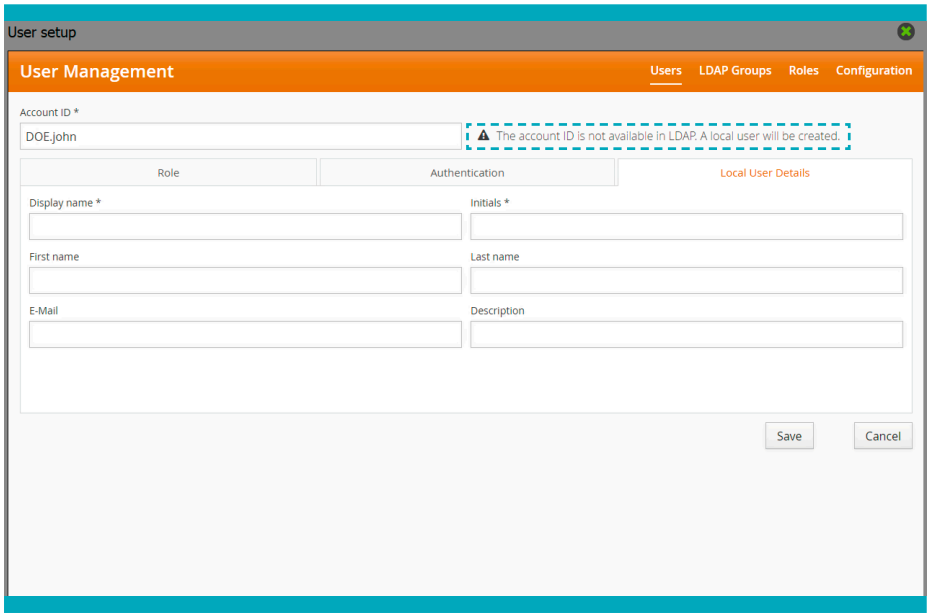
10.2.5 Add LDAP users

1. Go to <Users> in <User Management>.
2. Tap <+New User>.
3. Enter LDAP account ID. The software will check if this ID is registered in the AD server. If the user already exists, more information will be filled using the attribute mapping (see Screen 10.10). If the user is not registered in AD, a new local user will be created (see Screen 10.11).



Screen 10.10: User Management LDAP Users menu showing exemplarily a registered user

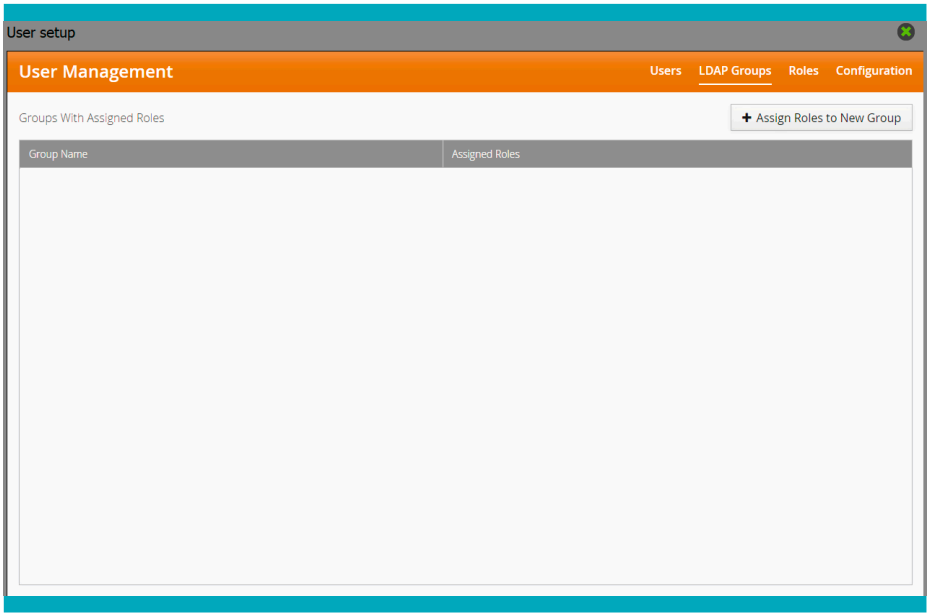
4. To assign roles tap <Role> and select the desired role.
5. Tap <save>. The user can use LDAP account ID and password to login.



Screen 10.11: User Management LDAP Users menu showing exemplarily a non-registered user

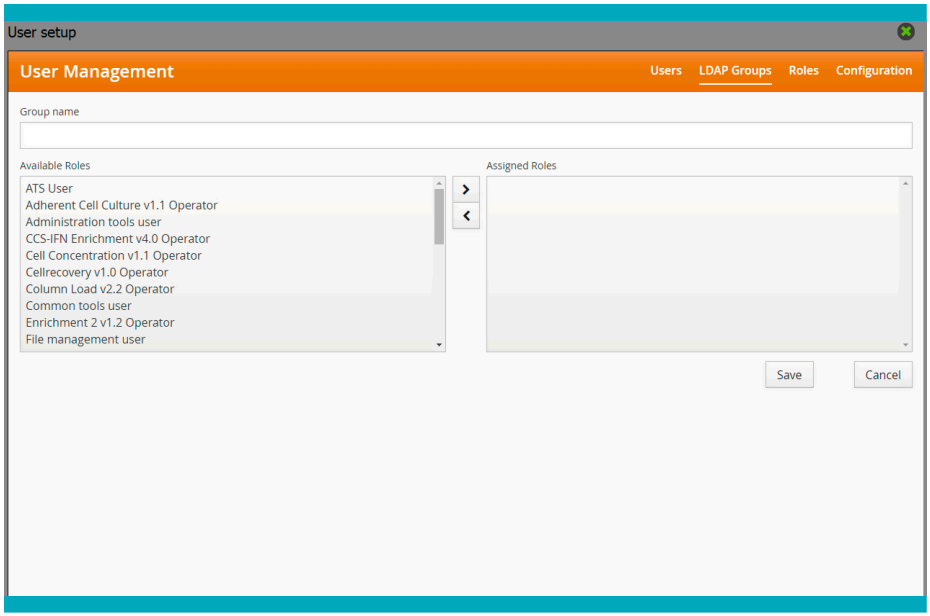
10.2.6 Add LDAP groups

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



Screen 10.12: User Management menu and the required step to add LDAP groups

2. Enter the group name (see Screen 10.13). The system will automatically check 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>.



Screen 10.13: User Management LDAP user groups menu

IMPORTANT

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

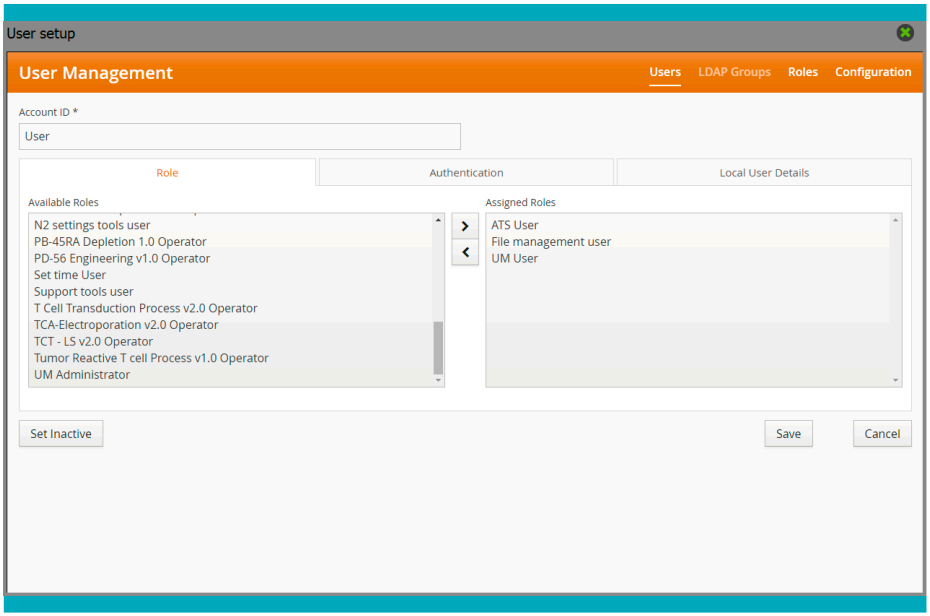
10.2.7 Change assigned roles of a user or LDAP group

1. Select user in the user list in the Users page (Screen 10.2) and tab the item. For LDAP group, select the desired group in LDAP groups page (Screen 10.12).
2. To assign additional roles to the user, 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 tab ‹.
3. Tap <Save> at the bottom of the <Role> tab.

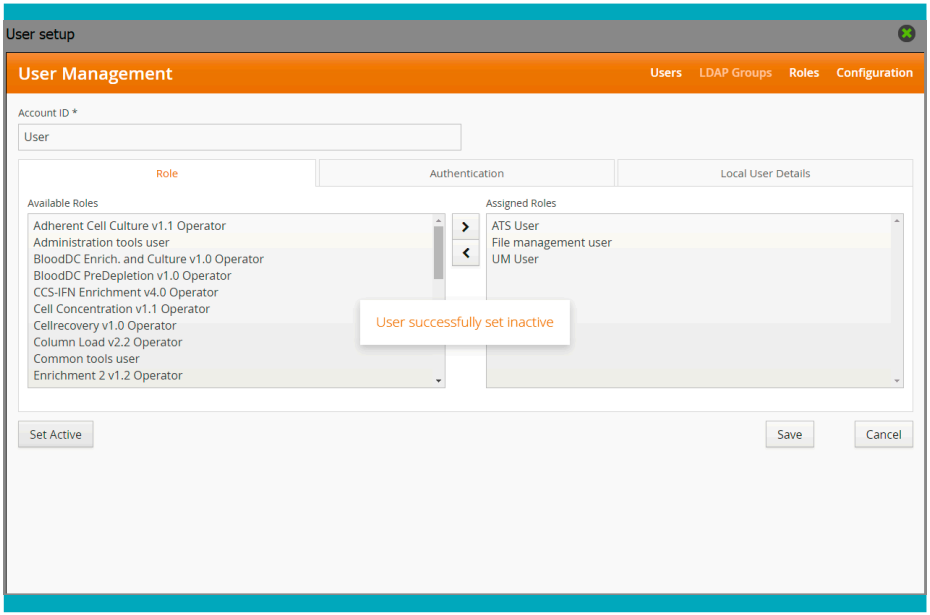
10.2.8 Deactivate local users

Note: Local user cannot be deleted, it can only be deactivated.

1. Select local user from user list (Screen 10.9). The user configuration page will be opened.
2. Tap <Set Inactive> at the bottom of the user configuration page (Screen 10.14).

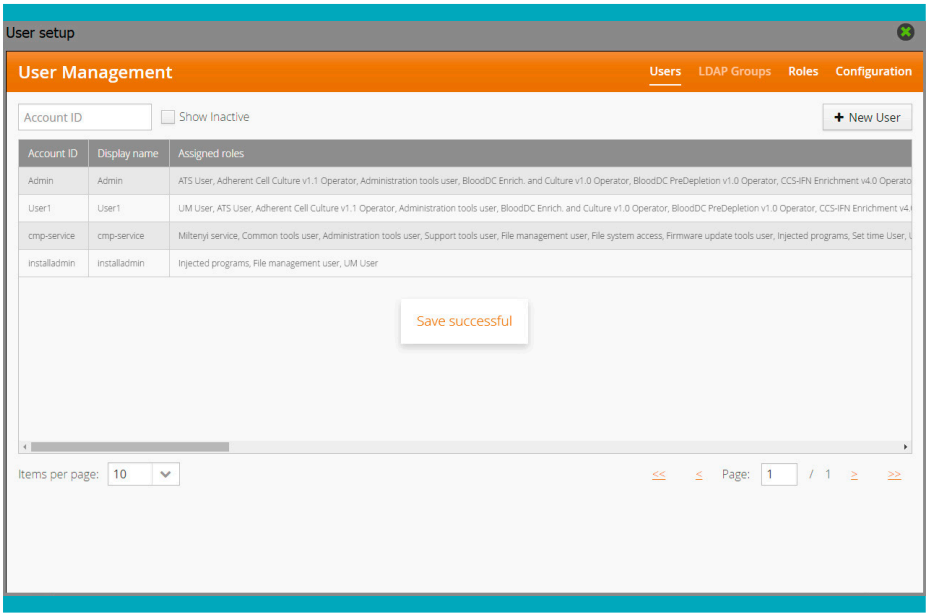


Screen 10.14: Set a local user inactive



Screen 10.15: User successfully set inactive

3. Tap <Save> at the bottom to return to the user list.

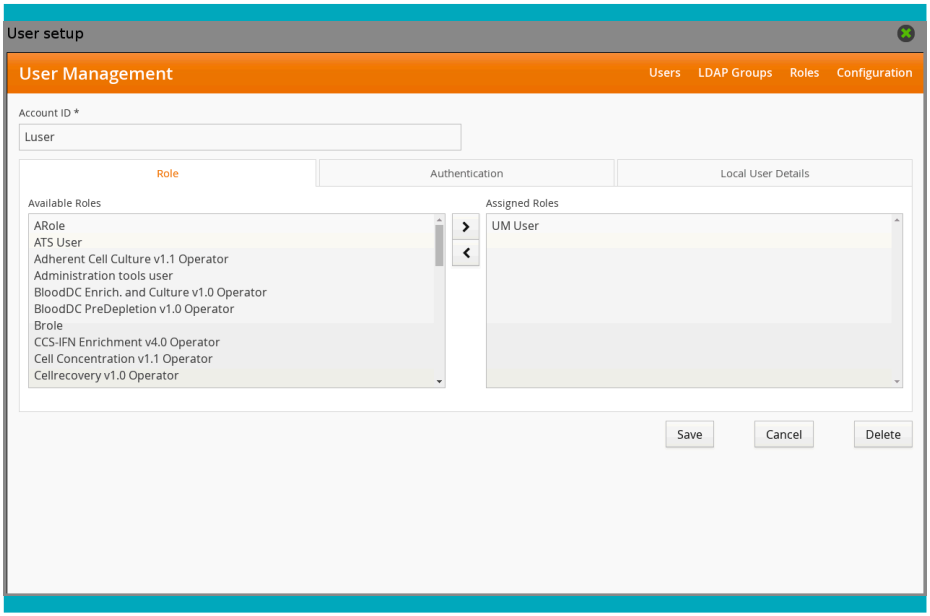


Screen 10.16: Saving successful

The inactive account will not be shown in the user list. Nevertheless the account is still stored on the instrument. To view or set this account active again, check <Show Inactive> (see Screen 10.16) and follow the same procedure in section 10.2.7 ´Change assigned roles of a user or LDAP group´.

10.2.9 Delete LDAP users

1. Select an LDAP user or LDAP group from the user list.
2. In the user configuration page, tap <Delete> (see Screen 10.17).



Screen 10.17: Delete LDAP User

3. Tap <Save> at the bottom to return to the user list.

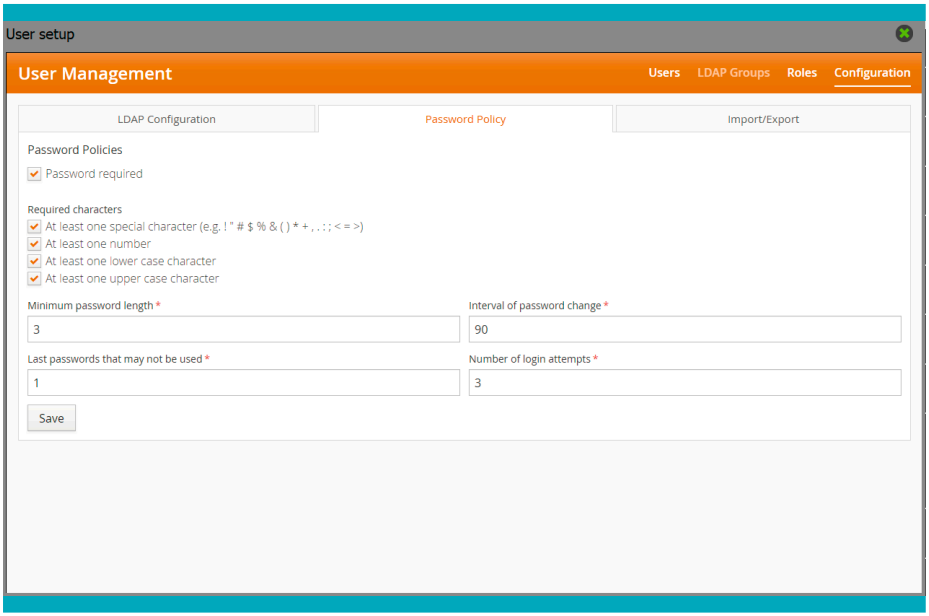
10.3 Configure password policy

To configure password policy, tap <Configuration> on the top right corner, select <Password Policy> tab. The following can be configured:

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

Note: Changing the password policy will only affect the users created afterwards. The already created users will not be affected.

Note: The password policy is overruled by the LDAP password policy for the LDAP account.



Screen 10.18: Configure password policy

10.4 Import and Export User Management settings

The UMS configuration can be transferred from one instrument to another. The process involves two stages:

(1) copy between USB flash drive and UMS exchange folder using UMS Exchange Tool

(2) Import/Export into UMS in the User Management Configuration.

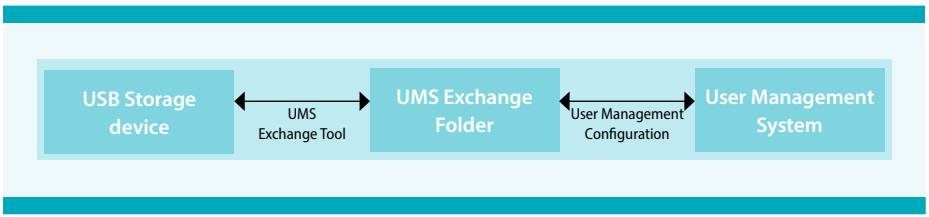


Figure 10.2: User Management System

The sample procedure applies for both of the following files:

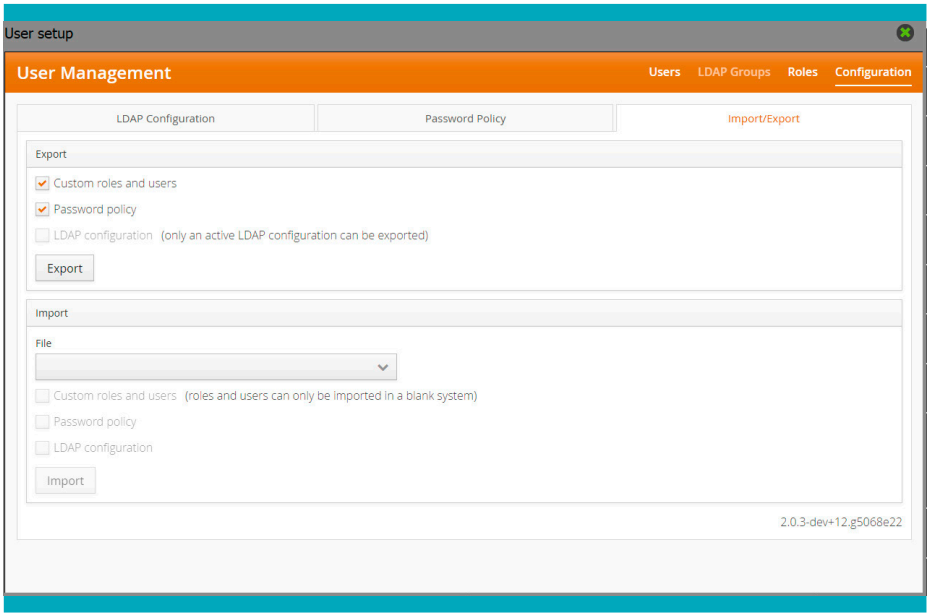
- Import Secure Sockets Layer (SSL) certificate files to set up a secure LDAP connection.
- Import and export UMS setting files for backup or reuse on other UMS instances.

Note: Only UMS users with the administrator role 'Administration tools user' will be able to access this application.

10.4.1 Export User Management settings

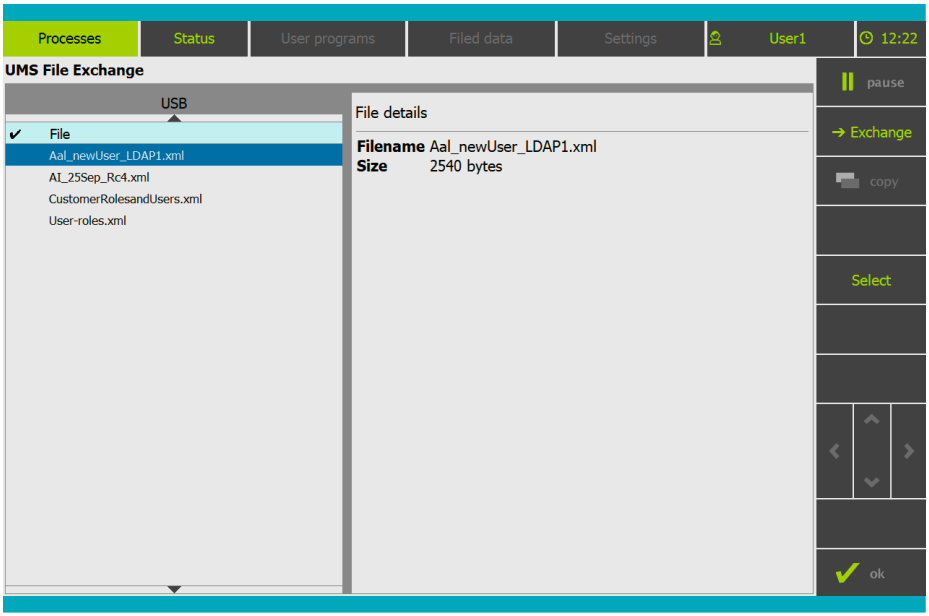
IMPORTANT
Roles and users can only be imported in a blank system.

1. Insert a USB flash drive.
2. Go to <User Management> ▸ <Configuration> ▸ <Import/Export>. Tap <Export>. The UMS settings are exported to UMS Exchange Folder on the instrument.



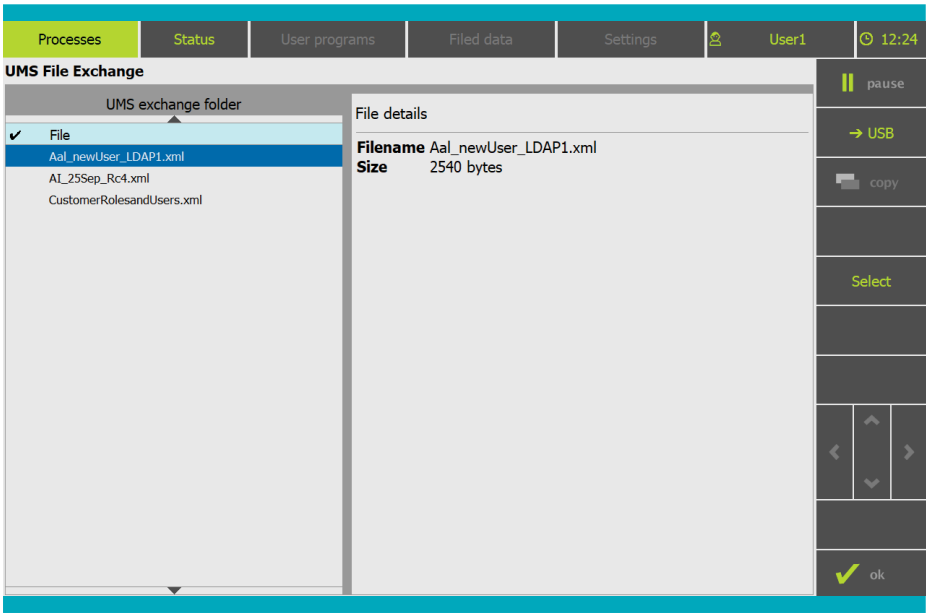
Screen 10.19: Submenu 'Configuration' with active 'Import/Export'

3. To enter the <UMS File Exchange>, go to <Settings> ▸ <Tools>, < UMS File Exchange>, and tap <run>.
4. If USB is shown on the left column, tap <Exchange> to list the contents of the UMS exchange folder (see Screen 10.20). The files in the UMS exchange folder will be shown in the left column (see Screen 10.21).



Screen 10.20: Selected file and menu button 'Exchange'

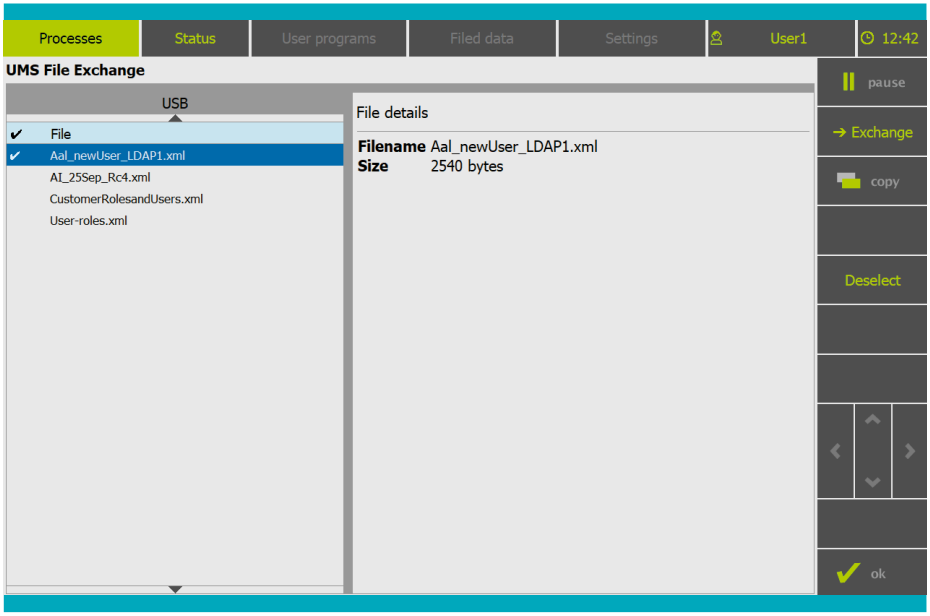
5. Select the files to be transferred to the UMS and tap <Select>.
6. Once all the files to be transferred are selected, tap <copy> to start the transfer.



Screen 10.21: UMS exchange folder with selected files

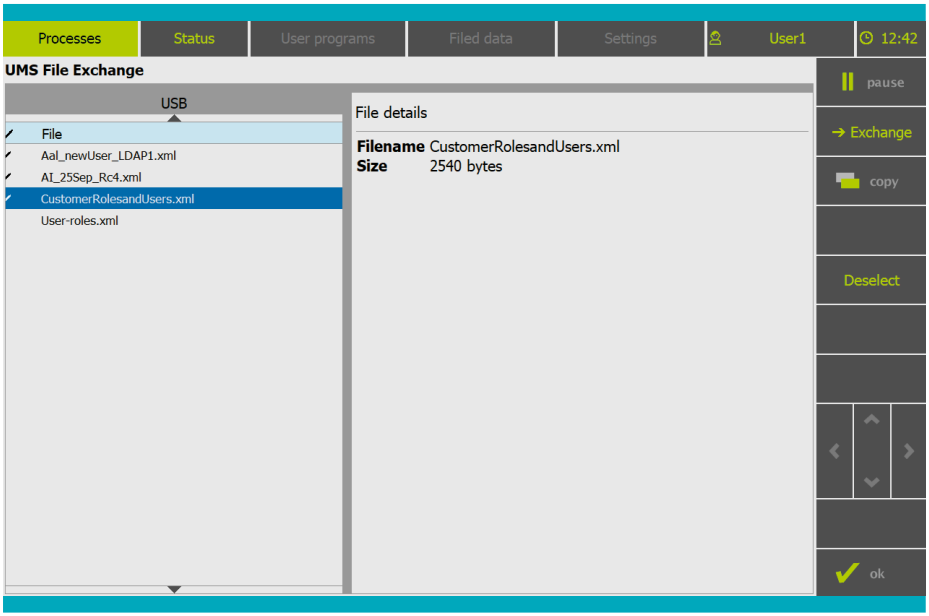
10.4.2 Import UMS settings

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>, 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>.



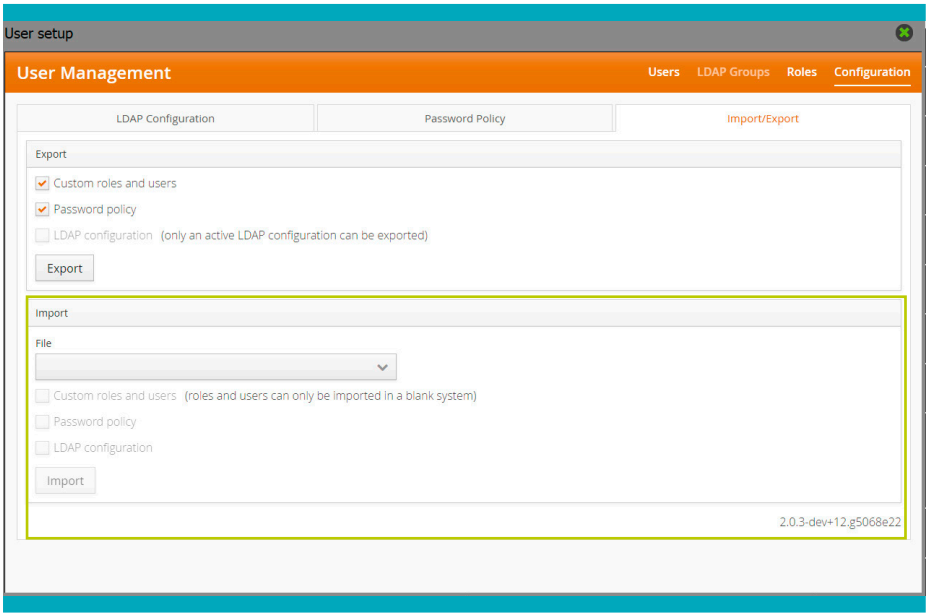
Screen 10.22: Selected file and menu button ‘Select

5. Once all the files to be transferred are selected, tap <Copy> to start transfer.



Screen 10.23: USB folder with selected files

6. Go to <User setup> ▸ <Configuration> ▸ <Import/Export>. Select the file in <Import> and tap <Import>.



Screen 10.24: Submenu 'Configuration' with active 'Import/Export' tab

11 Troubleshooting

In any case of instrument malfunction or process failure, contact the Miltenyi Biotec Technical Support at:

+49 2204 8306-3803
technicalsupport@miltenyi.com

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

12 Legal notes

12.1 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.

12.2 Trademarks

CliniMACS, CentriCult, and the Miltenyi Biotec logo are registered trademarks or trademarks of Miltenyi Biotec and/or its affiliates in various countries worldwide.

APPENDIX

Each process, tool and setting is associated with specific rights, e.g., 'Show' right and 'Start' right. With 'Show' right, the tool/process/setting will be visible in the Process /Settings tab. To be able to run the process/tool/setting, 'Start' right needs to be assigned to the role. More complicated components like audit trail and user management have more detailed rights.

Process/Tool/Settings/Component	Details
Process xxx right	• Show process xxx • Start process xxx
Tool xxx right • Backup Filed Data • Customer Files • Instrument check • License • N2 Settings • Network Settings • Set Time • Settings Exchange • SetVolume • Shutdown • UMSFileExchange exchange • UMSSettings settings Process xxx right	• Show tool xxx • Start tool xxx
Setting xxx right • Info • System settings	• Show setting xxx • Start setting xxx
Instrument	• Log file access via FTP • Show injected programs • Start injected programs
User Management	• Assign role • Configure LDAP connection • Create role • Create user • Export • Import • 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
Audit Trail Management	• Export audit trail events • Read audit trail events • Reset audit trail events

Table A.1: Overview of rights defined in the software

Default roles

Roles	Tools/rights
ATS User	User of the audit trail component • Audit trail Management
Administration tools user	• Customer settings • Network settings • Platform configuration settings • Settings exchange • System settings • UMSFileExchange exchange
File management user	A user that uses tools to manage files • Backup Filed Data • Custom Files • Log file access via FTP
File system access	Access to arbitrary executables in the file system – no access to rights
Support tools user	A user that can use tools that support the execution of applications • Chamber In • Chamber out • FormU Sensor • FormU Valves • FRAMrd • Gasmix Settings • Instrument Check • Module Settings • Sealer
UM Administrator	Administrator of the user management component User Management – all rights
UM Service	Service User • User Management – all rights
UM User	Customer User • User Management: Read details for own account • User Management: Read rights for own account

Table A.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.
Ground Floor,
Lab No. E 101/1,
Building no. 3600 | Plot No. 4,
Sy. no. 101, Neovantage Park,
Synergy Square 3 Genome
Valley, Lalgadimalakpet
Medchal Malkajgiri
Shamirpet (M)
Telangana 500101
India
+91 040 45175910
macsin@miltenyi.com

Italy
Miltenyi Biotec S.r.l.
Via Paolo Nanni Costa, 30
40133 Bologna
Italy
+39 051 6 460 411
+39 051 6 460 499
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

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

210-004-964/02 | Issued: 2026-01