Miltenyi Biotec

CliniMACS Prodigy® Software

Benutzerhandbuch



Die CliniMACS Systemkomponenten einschließlich Reagenzien, Schlauchsets, Instrumente und PBS/EDTA Puffer werden in einem nach ISO 13485 zertifizierten Qualitätssystem entworfen, hergestellt und geprüft In der EU sind die CliniMACS Systemkomponenten als Medizinprodukte mit CE-Kennzeichnung für ihre jeweilige Zweckbestimmung erhältlich, sofern nichts anderes angegeben ist. In den USA ist das CliniMACS CD34 Reagent System einschließlich dem CliniMACS Plus Instrument, dem CliniMACS CD34 Reagent, dem CliniMACS Tubing Set TS und CliniMACS Tubing Set LS sowie dem CliniMACS PBS/EDTA Buffer durch die FDA als Gerät zur Verwendung am Menschen (Humanitarian Use Device, HUD) und nach US-Bundesgesetz zur Behandlung von Patienten mit akuter myeloischer Leukämie (AML) in Erstremission zugelassen. Die Wirksamkeit des Geräts für diese Indikation ist nicht nachgewiesen. Andere Produkte der CliniMACS Produktlinie sind nur im Rahmen eines genehmigten Antrags auf Zulassung für die klinische Prüfung (Investigational New Drug Application, IND), auf den Ausnahmestatus für Studienzwecke (Investigational Device Exemption, IDE) oder im Rahmen einer FDA-Zulassung verfügbar. Die folgenden Komponenten sind im Australian Register of Therapeutic Goods (ARTG) registriert und damit für die Lieferung zugelassen: CliniMACS Prodigy, CliniMACS CD34 Reagent, CliniMACS Prodigy Tubing Sets und CliniMACS PBS/EDTA Buffer. Nur im ARTG registrierte Produkte dürfen in Australien verwendet werden. CliniMACS MicroBeads sind nur für Forschungszwecke und nicht für den therapeutischen oder diagnostischen Gebrauch am Menschen bestimmt.

Soweit nicht ausdrücklich anderweitig erwähnt, sind die Produkte und Dienstleistungen von Miltenyi Biotec nur für Forschungszwecke und nicht für therapeutische oder diagnostische Zwecke bestimmt.

Copyright © 2026 Miltenyi Biotec und/oder verbundene Unternehmen. Alle Rechte vorbehalten.

Diese Veröffentlichung darf ohne vorhergehende schriftliche Zustimmung seitens Miltenyi Biotec weder ganz noch in Auszügen und in keiner Form, sei es elektronisch, mechanisch, mittels Photokopie, Mikrofilm, Aufzeichnung oder mit sonstigen Mitteln vervielfältigt, in Datenabrufsystemen gespeichert, übertragen, veröffentlicht oder verbreitet werden. Eine Ausnahme hiervon gilt für Eigentümer des CliniMACS Prodigy Systems, wenn die angefertigten Kopien ausschließlich zur Schulung der Mitarbeiter in der Bedienung und Instandhaltung des Geräts innerhalb der eigenen Firma oder Organisation verwendet werden.

CliniMACS, CentriCult und das Miltenyi Biotec-Logo sind eingetragene Warenzeichen oder Warenzeichen der Miltenyi Biotec B.V. & Co. KG und/oder ihrer verbundenen Unternehmen in verschiedenen Ländern weltweit. Alle anderen in diesem Benutzerhandbuch oder in Begleitdokumenten genannten Warenzeichen sind Eigentum ihrer jeweiligen Inhaber und werden nur zu Identifikationszwecken verwendet.

CliniMACS Prodigy® Software

Benutzerhandbuch

Softwareversion 2.2

Stand: 2026-03

210-005-262/01

MD CE 0123

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

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

www.miltenyibiotec.com

Wichtige Informationen

Dieses Benutzerhandbuch enthält Anweisungen, Warnhinweise, Vorsichtsmaßnahmen, Hinweise und andere wichtige Informationen zur Anwendung der CliniMACS Prodigy Software. Weitere Informationen zu gerätespezifischen Themen wie Touchscreen und allgemeine Einrichtung finden Sie im Gerätehandbuch des CliniMACS Prodigy.

⚠ WARNUNG

Das CliniMACS Prodigy System darf nur von geschulten Anwendern bedient werden. Vor Inbetriebnahme des Systems ist es erforderlich, alle in den Gebrauchsanweisungen der einzelnen Systemkomponenten des CliniMACS Prodigy angegebenen Sicherheitshinweise, Warnhinweise, Vorsichtsmaßnahmen und Hinweise zum ordnungsgemäßen Betrieb des CliniMACS Prodigy sowie alle von Miltenyi Biotec veröffentlichten Sicherheitsempfehlungen sorgfältig gelesen und verstanden zu haben. Diese Gebrauchsanweisungen enthalten ohne Einschränkung die Sicherheitshinweise im Gerätehandbuch des CliniMACS Prodigy, Kapitel 3 'Wichtige Sicherheitshinweise'. Alle Warnhinweise, die auf dem Gerät angezeigt oder mit Verbrauchsmaterialien und Zubehörteilen mitgeliefert werden sowie alle in diesem Benutzerhandbuch beschriebenen Hinweise und wichtigen Informationen, sind besonders zu beachten. Befolgen Sie während des Betriebs dieses Geräts stets alle Anweisungen und Verfahrensweisen und stellen Sie sicher, dass alle Sicherheitshinweise, Warnhinweise, Vorsichtsmaßnahmen und Anweisungen beachtet werden. Die Missachtung der Sicherheitshinweise und wichtigen Informationen, Warnhinweise, Vorsichtsmaßnahmen, zusätzlichen Hinweise und Bedienhinweise in den Gebrauchsanweisungen kann zu Funktionsstörungen des Geräts, Sachschäden, Verletzungen und/oder zum Tod führen. Die Gerätesicherheit kann beeinträchtigt werden, wenn das Gerät nicht gemäß den Anweisungen des Herstellers verwendet wird. Bewahren Sie die Gebrauchsanweisungen für spätere Nachschlagezwecke auf. Sie sollten zusammen mit allen anderen Sicherheits- und Bedienungsunterlagen während der gesamten Lebensdauer des Geräts für alle, die mit Installation, Betrieb und Wartung des Geräts betraut sind, griffbereit und leicht zugänglich aufbewahrt werden.

Inhaltsverzeichnis

1	**Einführung**	**9**
1.1	Allgemeine Informationen	9
1.2	Regulatorische Hinweise	10
1.3	Datenschutzbestimmungen	10
1.4	Über dieses Handbuch	11
1.5	Zugehörige Dokumente	11
2	**Glossar**	**13**
2.1	Gefährdungsgrad	13
2.2	Darstellungskonventionen	14
2.3	Glossar der Symbole und Fachbegriffe	14
2.3.1	Software-spezifische Begriffe	15
3	**Wichtige Sicherheitshinweise**	**17**
3.1	Sicherheitsanweisungen für den CliniMACS Prodigy	17
3.2	Sicherheitsanweisungen für die Software	17
4	**Cyber-Sicherheit**	**19**
4.1	Defense-in-depth-Strategie für mehr Sicherheit	19
4.1.1	Physische Schutzebene	20
4.1.2	Ebene der Netzwerkumgebung	21
4.1.3	Ebene der Gerätesoftware	24
4.1.4	Benutzerebene	25
4.1.5	Audit-Trail-Ebene	25
4.1.6	Ebene des Update-Handlings	26
4.1.7	Ebene des Handlings von Sicherheitslücken	26
4.1.8	Ebene der Datensicherung und Wiederherstellung	26
4.1.9	Zusammenfassung der sicheren Konfiguration	27

5	**Softwarekonzept**	**29**
5.1	Grundkonzept	29
5.2	Grafische Benutzeroberfläche	30
5.2.1	Menüleiste und Inhaltsbereich	31
5.2.2	Statuszeile	32
5.2.3	Werkzeugleiste	32
5.2.4	Eingabefelder	34
5.2.5	Pop-up-Fenster	35
6	**Grundlegender Betrieb**	**37**
6.1	Einschalten des Geräts	37
6.2	Login	38
6.3	Logout (Abmelden)	39
6.4	Abschalten	39
6.5	Not-Aus-Funktion	39
6.6	Wählen eines Anwendungsprozesses	40
6.7	Ausführen eines Anwendungsprozesses	41
6.8	Anhalten eines Anwendungsprozesses	42
6.9	Gerätestatus und Status des Anwendungsprozesses	43
6.10	Aufnehmen von Bildern	44
6.10.1	Layer Detection Camera	45
6.10.2	Mikroskopkamera	46
7	**Datenzugriff**	**49**
7.1	Abrufen von Anwendungsprotokollen	49
7.1.1	Anzeigen und Exportieren von Protokolldateien auf einen USB-Stick	49
7.1.2	Abrufen über FTP	51
7.1.3	Abrufen von Dateien über File Sharing	52
7.2	Abrufen des Audit-Trails	53
7.2.1	Anzeigen des Audit-Trails	54
7.2.2	Exportieren des Audit-Trails	55
7.2.3	Löschen des Audit-Trails	57

8	**Tools und Benutzereinstellungen**	**59**
8.1	Zugriff auf Tools und Benutzereinstellungen	59
8.2	Tools	60
8.2.1	Info tool	60
8.2.2	Backup Filed Data (Datensicherung für Dateien)	61
8.2.3	Chamber In (Kammer rein)	65
8.2.4	Chamber Out (Kammer raus)	65
8.2.5	Shutdown	66
8.2.6	Recovery (Rückgewinnung)	66
8.2.7	Gas Mix tool (Gasmisch-Tool)	66
8.2.8	Instrument Check tool (Geräteprüfung)	67
8.2.9	Column Load (Säulenbeladung)	67
8.2.10	Custom Files (benutzerdefinierte Dateien)	67
8.2.11	Sealer (Schlauchschweißgerät)	67
8.3	User settings (Benutzereinstellungen)	67
8.3.1	Set time (Uhrzeit einstellen)	67
8.3.2	Network settings (Netzwerkeinstellungen)	67
8.3.3	Custom settings (Benutzerdefinierte Einstellungen)	68
8.3.4	Module Settings (Einstellungen für die Module)	68
8.3.5	Tool Settings Exchange (Austausch von Einstellungen)	69
8.3.6	SetVolume (Volumen einstellen)	73
8.3.7	N_2 Settings (N_2-Einstellungen)	73
9	**Netzwerkintegration**	**75**
9.1	Verbinden mit einem lokalen Netzwerk	76
9.2	Verbindung zu einem LDAP-Server herstellen	78
9.3	Verbindung zu einem Netzlaufwerk herstellen	81
9.4	Konfigurieren der Dateiübertragung über FTP	84
9.4.1	Einrichten des Geräts	85
9.4.2	Verbinden mit FTP-Client	86
9.5	Verbinden mit einem E-Mail-Server	87
9.6	Aktivieren der Netzwerk-Zeitsynchronisation	93

10 Benutzerverwaltung 95
10.1 Allgemeine Informationen 95
10.2 Verwalten von Rollen und Konten 98
10.2.1 Zugriff auf die Benutzerverwaltung 98
10.2.2 Erstellen einer neuen Rolle 99
10.2.3 Ändern der Rechte von Rollen 100
10.2.4 Hinzufügen eines lokalen Benutzers 101
10.2.5 Hinzufügen von LDAP-Benutzern 104
10.2.6 Hinzufügen von LDAP-Gruppen 106
10.2.7 Ändern der zugewiesenen Rollen eines Benutzers oder einer LDAP-Gruppe 107
10.2.8 Deaktivieren lokaler Benutzer 107
10.2.9 Löschen von LDAP-Benutzern 109
10.3 Konfigurieren der Passwortrichtlinien 110
10.4 Import und Export von Einstellungen für das User Management 111
10.4.1 Exportieren der Einstellungen der Benutzerverwaltung 112
10.4.2 Importieren von UMS-Einstellungen 114

11 Fehlerbehebung 117

12 Rechtliche Hinweise 119
12.1 Beschränkte Garantie 119
12.2 Marken 120

ANHANG

1 Einführung

1.1 Allgemeine Informationen

Die Software auf dem CliniMACS Prodigy besteht aus einer Kernsoftware und verschiedenen anwendungsspezifischen Softwareprogrammen.

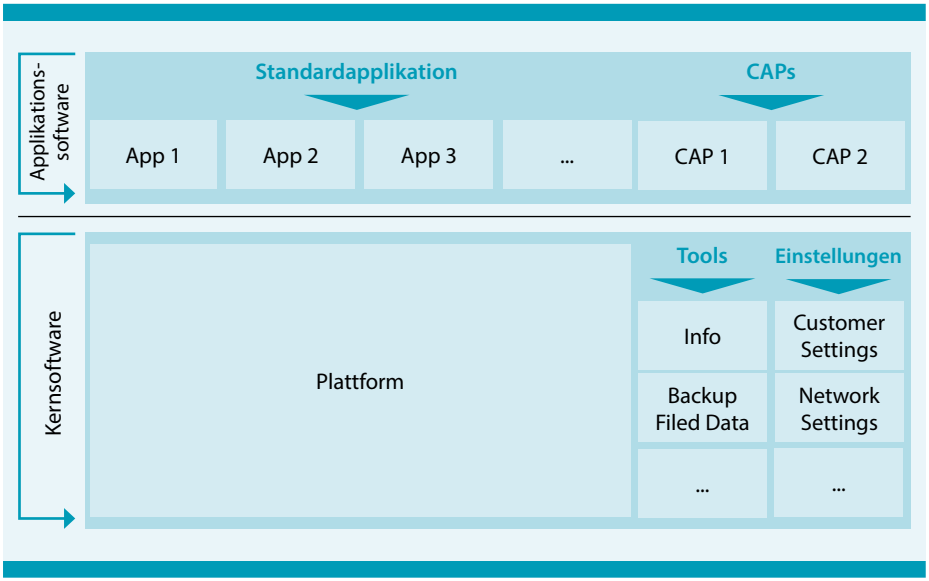


Abbildung 1.1: Übersicht über die Geräte-Software

Die Kernsoftware steuert das Gerät und die Ausführung von Anwendungsverfahren und stellt grundlegende Dienste bereit, die in den verschiedenen Kapiteln und Abschnitten beschrieben werden.

Die Kernsoftware wird in diesem Benutzerhandbuch auch als Software bezeichnet.

Die Anwendungssoftware wird von der Kernsoftware ausgeführt und stellt die Anwendungsverfahren und Benutzerschnittstellen für den Betrieb des CliniMACS Prodigy je nach Verwendungszweck bereit:

- als Teil des CliniMACS Prodigy Zellseparationsystems zur Separation humaner Zellen
- als Teil des CliniMACS Prodigy Produktionssystem für Zell- und Gentherapeutika zur genetischen und/oder sonstigen substanziellen Bearbeitung (wie etwa Proliferation und Differenzierung) humaner Zellen

Die Kernsoftware und alle Anwendungen sind unabhängige Module, sodass eine neue Anwendung separat hinzugefügt werden kann, ohne die Kernsoftware zu ändern.

1.2 Regulatorische Hinweise

Die Software wurde entsprechend der Norm IEC/EN 62304 entwickelt. Darüber hinaus wurde die CliniMACS Prodigy Kernsoftware entwickelt, um die Einhaltung von GAMP 5, EudraLex Band 4 Anhang 11 (EU GMP Anhang 11) und 21 CFR Teil 11 zu unterstützen.

Die Anforderungen an die Cyber-Sicherheit werden gemäß der Norm IEC 81001-5-1 erfüllt, einschließlich der von einem Drittunternehmen durchgeführten Penetrationstests.

Die vollständige Übersicht über die regulatorischen Informationen einschließlich der beabsichtigten Verwendung ist Teil des Gerätehandbuchs des CliniMACS Prodigy.

1.3 Datenschutzbestimmungen

Bei der Verarbeitung personenbezogener Daten mit dem CliniMACS Prodigy System sollten Benutzer äußerst umsichtig vorgehen. Der Benutzer ist für die Einhaltung der geltenden Datenschutzgesetze und -vorschriften verantwortlich. In Übereinstimmung mit den Grundsätzen des Datenschutzes hat Miltenyi durch technische und datenschutzfreundliche Voreinstellungen Sicherheitsmaßnahmen umgesetzt, insbesondere die Defense-in-Depth-Strategie (siehe Abschnitt 4.1 ‘Defense-in-depth-Strategie für mehr Sicherheit’).

1.4 Über dieses Handbuch

Dieses Benutzerhandbuch enthält die erforderlichen Informationen für die Einrichtung und den sicheren Betrieb der Kernsoftware. Nur die Kernsoftware 2.2 ist im Umfang dieses Benutzerhandbuchs enthalten.

1.5 Zugehörige Dokumente

Das Gerätehandbuch des CliniMACS Prodigy beschreibt die Hardware und das System des CliniMACS Prodigy Geräts. Das Benutzerhandbuch für das Gerät wird zusammen mit diesem Handbuch bereitgestellt.

Das Benutzerhandbuch für das Gerät enthält:

- Warnungen, Vorsichtsmaßnahmen und Hinweise
- Regulatorische Hinweise
- Technische Daten
- Weitere wichtige Informationen

Bei Verwendung des CliniMACS Prodigy zusammen mit dem MACS® TubeSealer, dem CliniMACS Electroporator, der CliniMACS Formulation Unit oder der CliniMACS Workbench sind folgende zugehörige Benutzerhandbücher zu beachten:

- MACS TubeSealer Benutzerhandbuch
- CliniMACS Electroporator Benutzerhandbuch
- CliniMACS Formulation Unit Benutzerhandbuch
- CliniMACS Workbench Benutzerhandbuch

Eine vollständige Übersicht über die verfügbaren Zubehörteile, Komponenten und MACS GMP-Geräte finden Sie im Gerätehandbuch des CliniMACS Prodigy.

Für Informationen zu bestimmten Anwendungen wenden Sie sich bitte an den Miltenyi Biotec Technical Support.

2
Glossar

2.1 Gefährdungsgrad

Die Farbe und das Signalwort einer Warnmeldung hängen vom Gefährdungsgrad ab. Die unten beschriebenen Gefährdungsstufen klassifizieren die Gefahr. Schwere, Art und Ursprung der Gefahr sowie mögliche Folgen, Verbote und Vorsichtsmaßnahmen werden nachfolgend beschrieben.

⚠ WARNUNG

Weist auf eine Gefahrensituation hin, die schwere Verletzungen oder den Tod zur Folge haben kann, wenn sie nicht vermieden wird.

⚠ VORSICHT

Weist auf eine Gefahrensituation hin, die leichte oder mittelschwere Verletzungen zur Folge haben kann, wenn sie nicht vermieden wird.

ACHTUNG

Weist auf Informationen hin, die als wichtig erachtet werden, aber nicht im Zusammenhang mit einer Gefährdung stehen (z. B. Hinweise auf Sachschäden).

WICHTIG

Weist den Anwender auf wichtige Verfahrensweisen oder Informationen hin, die sich weder auf Körperverletzungen noch Sachschäden beziehen.

2.2 Darstellungskonventionen

Text in **<hellgrün>** kennzeichnet Elemente in der grafischen Benutzeroberfläche (z. B. Schaltflächen, Dialogfelder oder Elemente der Benutzerverwaltung).

2.3 Glossar der Symbole und Fachbegriffe

Eine Übersicht über die für das CliniMACS Prodigy System verwendeten Symbole und allgemeinen Begriffe ist im Gerätehandbuch des CliniMACS Prodigy zu finden. Das Glossar der Symbole erklärt alle Symbole, die auf den CliniMACS® Produkten zur Kennzeichnung verwendet werden.

2.3.1 Software-spezifische Begriffe

Anwendungsprozess	Von Miltenyi Biotec entwickelte Software für die Zellverarbeitung
ATS Audit Trail System	Eine Softwarekomponente, die Ereignisse, Aktionen, Benutzereingaben und Änderungen innerhalb der CliniMACS Prodigy Software verfolgt und aufzeichnet
CAP	Kundenspezifischer Anwendungsprozess (Customized Application Process)
FTP File Transfer Protocol	Standard-Kommunikationsprotokoll, das für die Übertragung von Computerdateien von einem Server zu einem Client in einem Computernetzwerk verwendet wird
LDAP Lightweight Directory Access Protocol	Anwendungsprotokoll für den Zugriff auf und die Pflege verteilter Verzeichnisinformationsdienste über ein Internet-Protokoll-Netzwerk
MD5	Algorithmus zur Erstellung von Prüfsummen, um die Datenintegrität vor unbeabsichtigter Schädigung zu schützen
Prozess für Standardapplikationen	Ein vorab von Miltenyi Biotec validierter Applikationsprozess
SMB Server Message Block	Kommunikationsprotokoll zur gemeinsamen Nutzung von Dateien, Druckern, seriellen Anschlüssen sowie verschiedene Kommunikationen zwischen den Knoten eines Netzwerks
SMTP Simple Mail Transfer Protocol	Kommunikationsprotokoll für die E-Mail-Übertragung

UMS User Management System (Benutzerverwaltung)	Eine Softwarekomponente zur Verwaltung und Steuerung des Benutzerzugriffs auf die verschiedenen Funktionen des Geräts

3

Wichtige Sicherheitshinweise

3.1 Sicherheitsanweisungen für den CliniMACS Prodigy

Detaillierte Informationen zur Sicherheit des Geräts finden Sie im Gerätehandbuch des CliniMACS Prodigy.

3.2 Sicherheitsanweisungen für die Software

WICHTIG

Die Zugangskontrolle des Geräts muss vor Gebrauch validiert werden. Benutzername und Passwort sind sicher zu verwahren. Es wird empfohlen, einen Notfallzugriff einzurichten (siehe Kapitel 10 ´Benutzerverwaltung´). Im Falle einer fehlgeschlagenen Anmeldung während eines laufenden Prozesses kontaktieren Sie den Miltenyi Biotec Technical Support.

- Lesen Sie vor der Verwendung des Geräts mit der Softwareversion 2.2 das Kapitel 3 „Wichtige Sicherheitshinweise“ im Gerätehandbuch des CliniMACS Prodigy sowie alle anderen Informationen in diesem Software-Benutzerhandbuch, einschließlich aller Sicherheits- und Betriebsanweisungen.
- Alle Warnhinweise, die auf dem Gerät angezeigt werden, sind besonders zu beachten.
- Werden diese Richtlinien nicht gelesen und befolgt, kann dies zu unsachgemäßem oder falschem Gebrauch und zu Schäden am Gerät führen. Eine unsachgemäße Verwendung kann auch zu schweren Verletzungen, Tod, unvorhersehbaren Ergebnissen, Fehlfunktionen des Geräts und vorzeitigem Verschleiß von Komponenten führen, die die Lebensdauer des Geräts

verkürzen. Derartige Vorgehensweisen können zum Erlöschen der Garantie führen.

- Für spätere Nachschlagezwecke sollten das Benutzerhandbuch und alle anderen, mit dem Gerät gelieferten Sicherheits- und Betriebsanweisungen an einem sicheren, für alle Benutzer zugänglichen Ort aufbewahrt werden.
- Alle Verarbeitungsverfahren dürfen nur von geschulten Anwendern durchgeführt werden. Anwender müssen ein allgemeines Verständnis der Zellverarbeitung und Wissen über Biosicherheit haben.
- Nur von Miltenyi Biotec autorisierte örtliche Servicedienstleister dürfen das Gerät installieren oder warten.
- Die Kommunikation und der Datenzugriff zwischen der Software und einem externen Server bzw. einer externen Anwendung müssen vor der Verwendung des Geräts validiert werden.
- Wenden Sie sich bei ernsthaften Bedenken hinsichtlich der sicheren Verwendung des Geräts an den Miltenyi Biotec Technical Support.
- Im Falle von Problemen oder Störungen wenden Sie sich an den Miltenyi Biotec Technical Support.

4

Cyber-Sicherheit

4.1 Defense-in-depth-Strategie für mehr Sicherheit

Die Cyber-Sicherheit liegt in der gemeinsamen Verantwortung von Miltenyi Biotech und den Benutzern. Die Software enthält integrierte Sicherheitsmaßnahmen zum Schutz vor den häufigsten Bedrohungen. Die Benutzer müssen eine aktive Rolle beim Schutz der Daten und Einhaltung sicherer Verfahren spielen. In Übereinstimmung mit der bestimmungsgemäßen Verwendung wird ein Defense-in-Depth-Modell empfohlen. Das Ziel dieses Defense-in-Depth-Modells ist:

- Vermeidung negativer Auswirkungen auf die Qualität der Zellprodukte und Vermeidung von Verzögerungen der Zellprodukte
- Die Integrität von Protokollen, Prozessen und Audit-Trail-Daten
- Die Integrität der Systemkonfiguration
- Die Verfügbarkeit des Geräts für die Zellverarbeitung
- Nur geschulten und berechtigten Anwendern den Zugriff auf das Gerät zu erlauben

Das Defense-in-Depth-Modell ist in folgende Ebenen gegliedert:

- Physische Schutzebene
- Ebene der Netzwerkumgebung
- Ebene der Gerätesoftware
- Benutzerebene
- Audit-Trail-Ebene
- Ebene des Update-Handlings
- Ebene des Handlings von Sicherheitslücken
- Ebene der Datensicherung und Wiederherstellung

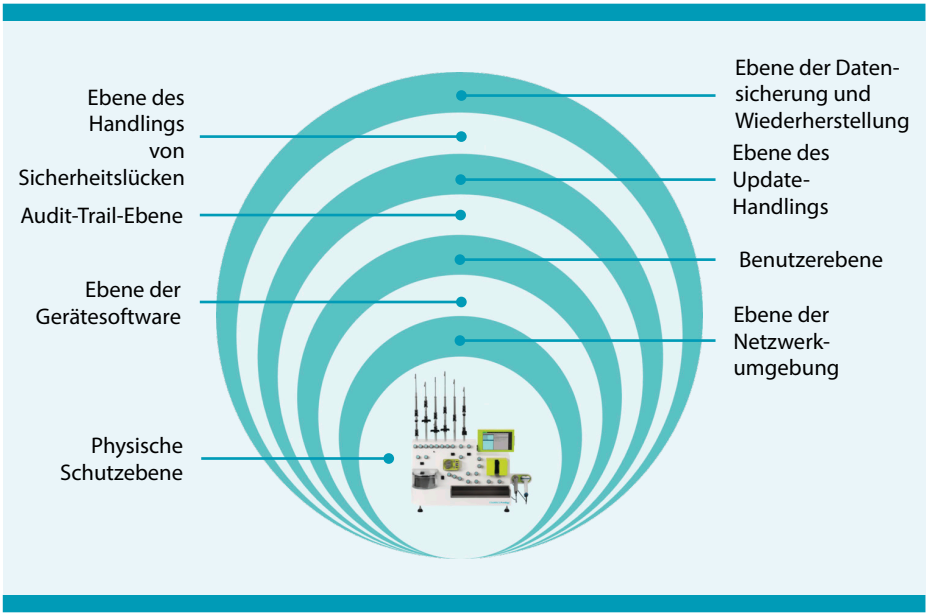


Abbildung 4.1: Ebenen der Defense-in-Depth-Strategie

4.1.1 Physische Schutzebene

Das Gerät ist mit den folgenden physischen Schnittstellen ausgestattet, die den Anschluss der verschiedenen Komponenten, Zubehörsysteme und Geräte unterstützen (siehe Tabelle 4.1).Der Kunde ist dafür verantwortlich, dass nur berechtigtes Personal einen physischen Zugang zum Produkt erhält, und muss geeignete Prozesse zur Kontrolle und Überwachung des physischen Zugangs einrichten.

Schnittstelle	Zweck
USB-Anschluss	Anschließen zulässiger Peripheriegeräte an das Gerät, wie zum Beispiel die externe Tastatur oder das Barcode-Lesegerät. Über einen USB-Ethernet-Adapter kann das Gerät mit dem Netzwerk verbunden werden. Über USB-Sticks können Protokolle, Bilder und Protokolldateien vom Gerät übertragen und Programme/Updates im Gerät installiert werden. Auch zur Installation des Geräts werden USB-Sticks genutzt.
Touchscreen	Ein Dateneingabegerät, das von Anwendern des Geräts sowie von Wartungs- und Servicepersonal verwendet wird.
CAN-Bus/Power CAN-Schnittstelle	Diese Schnittstelle dient zum Anschließen zusätzlicher Geräte, wie zum Beispiel des CliniMACS Electroporators oder der CliniMACS Formulation Unit, an das Gerät.
Sealer-Anschluss	Versorgt den MACS TubeSealer, ein am CliniMACS Prodigy angeschlossenes Schlauchschweißgerät, mit Strom. Keine Datenschnittstelle.
Alarmanschluss	Relaisschalter-Anschluss zur Verbindung des Geräts mit einem externen Alarmsystem. Keine Datenschnittstelle.

Tabelle 4.1: Schnittstellen und Peripheriegeräte des Geräts

Die USB-Anschlüsse ermöglichen den Anschluss von USB-Sticks. Es sind zwar Schutzmaßnahmen im Betriebssystem und auf der Applikationsebene zur Kontrolle der USB-Anschlüsse eingerichtet, aber es liegt in der Verantwortung des Kunden, sicherzustellen, dass nur zulässige und kontrollierte USB-Sticks mit dem Gerät verwendet werden.

Anmerkung: Es werden nur USB-Sticks im FAT32-Format unterstützt.

Eine unsachgemäße Handhabung von Schnittstellen oder Zubehörteilen (z. B. gewaltsames Anschließen von Steckverbindern) kann die Anschlüsse des Geräts beschädigen, sodass sie nicht mehr funktionieren und ein Restrisiko darstellen.

4.1.2 Ebene der Netzwerkumgebung

Das Gerät sollte in einem geschützten Netzwerksegment, das von anderen Netzwerkbereichen getrennt ist, betrieben werden. Ein mögliches Setup, in dem das Gerät Teil eines isolierten Gerätenetzwerks ist, sehen Sie in Abbildung 4.2. Ein Router trennt die verschiedenen Netzwerksegmente voneinander und steuert den Datenfluss zwischen ihnen.

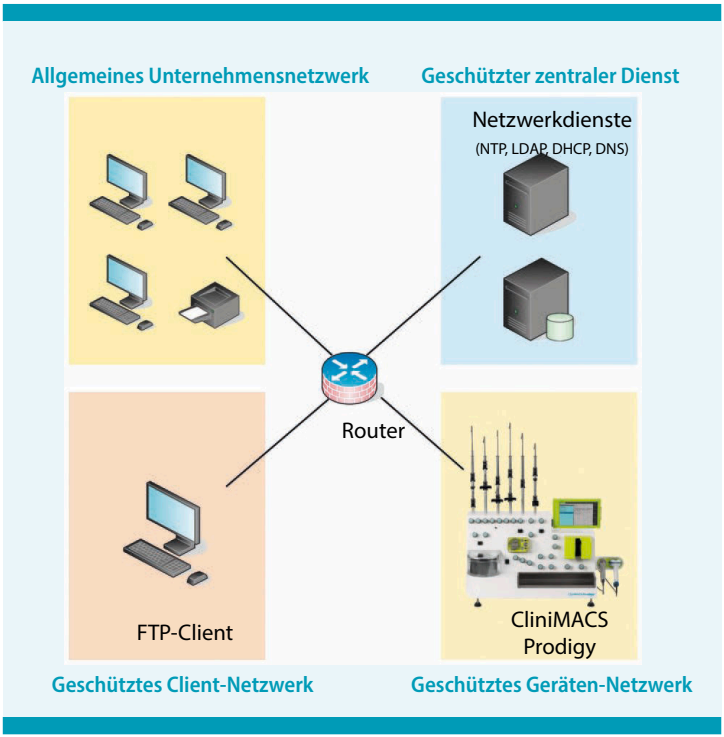


Abbildung 4.2: Netzwerkdiagramm

Das Gerät stellt hauptsächlich Funktionen zum Anschließen an andere Systeme im Netzwerk bereit. Die unterstützten Netzwerkprotokolle zeigt Tabelle 4.2.

Schnittstelle	Zweck	Anschluss	Kommentar
FTP	Nur-Lesen-Zugriff auf Protokolldateien über FTP	20 – 21	Über FTP können die Protokolldateien und Passwörter in Klartext über das Netzwerk übertragen werden. Es wird empfohlen, für den Zugriff auf Daten über FTP eigens ein Benutzerkonto einzurichten, um das Risiko für den FTP-Dienst zu minimieren und Seitwärtsbewegung zu verhindern, falls das Benutzerkonto kompromittiert wird. Standardmäßig ist FTP deaktiviert.
NTP	Zeitsynchronisation	123	–
DNS (Client)	Auflösen von Host-Namen für IP-Adressen	53 (UDP)	–

Schnittstelle	Zweck	Anschluss	Kommentar
ICMP-Echo-Request/ Response (Server)	Netzwerkverbindung zum Gerät überprüfen	N/A	–
DHCP (Client)	Die automatische Netzwerkkonfiguration des Geräts	68 (UDP)	–
LDAP	Anmeldung am Gerät mit zentral verwalteten Active-Directory-Zugangsdaten	389	Unsicheres Protokoll, nur verwenden, wenn LDAPS nicht unterstützt wird
LDAPS	Gesicherte LDAP-Version	636	Eine sichere LDAP-Variante. Erfordert eine ordnungsgemäße Konfiguration, siehe Abschnitt 9.2 ´Verbindung zu einem LDAP-Server herstellen´.
SMB	File Sharing	445	Authentifizierter Austausch wird unterstützt. Erfordert eine Konfiguration, siehe Abschnitt 9.3 ´Verbindung zu einem Netzlaufwerk herstellen´
SMTP	E-Mail-Benachrichtigung	25, 2525, 465, 587	Authentifizierung wird unterstützt. Erfordert eine ordnungsgemäße Konfiguration, siehe Abschnitt 9.5 ´Verbindung zu einem E-Mail-Server herstellen´
SMTPS	Gesicherte SMTPS-Version	465, 587	Eine sichere SMTP-Variante. Erfordert eine ordnungsgemäße Konfiguration, siehe Abschnitt 9.5 ´Verbinden mit einem E-Mail-Server´

Tabelle 4.2: Netzwerkverbindungen und -protokolle

WICHTIG

Mit Ausnahme von FTP werden für alle Dienste sichere Protokolle unterstützt. Es wird dringend geraten, nur die in Tabelle 4.2 aufgeführten sicheren Funktionen zu aktivieren.Aus Gründen der Kompatibilität werden unsichere Versionen von Protokollen nicht unterstützt. In Fällen, in denen aus Kompatibilitätsgründen das unsichere Protokoll benötigt wird, müssen vom Kunden geeignete Maßnahmen zur Risikominimierung getroffen werden.

Der Kunde ist dafür verantwortlich, sicherzustellen, dass nur autorisiertes Personal einen Netzwerkzugang zum Gerät und zu den Netzwerken hat, die zur Übertragung der aktivierten Protokolle verwendet werden. Es müssen geeignete Prozesse zur Kontrolle und Überwachung des Netzwerkzugangs eingerichtet sein. Außerdem darf das Gerät nicht direkt über das Internet zugänglich sein.

4.1.3 Ebene der Gerätesoftware

Ein kundenspezifisches Linux-Betriebssystem läuft auf dem Gerät. Nur absolut notwendige Software, Dienste und Kernel-Features sind aktiviert, um die Angriffsfläche der Gerätesoftware zu minimieren.

Der Zugriff auf das BIOS des Geräte-PCs steht nur von Miltenyi geschultem Servicepersonal zur Verfügung. Die Konfiguration des BIOS verhindert ein Booten von externen Medien, um die Integrität der Gerätesoftware sicherzustellen.

Es sind Vorkehrungen getroffen, die sicherstellen, dass nur zulässige Software auf dem Gerät betrieben werden kann. Neue Software wird mithilfe eines USB-Sticks auf dem Gerät installiert. Der automatische Start von Software vom USB-Stick wird verhindert, und Applikationen können nicht direkt von einem USB-Stick gestartet werden.

Zusätzliche Software, die auf dem Gerät allgemein verfügbar sein soll, muss mit einem Installer, der mit dieser Software geliefert wird, installiert werden. Um sicherzustellen, dass nur die Originalsoftware von Miltenyi Biotec, die für das Gerät vorgesehen ist, installiert werden kann, sind mehrere Kontrollen eingerichtet. So prüft der Installer das Ablaufdatum des Installationspakets sowie die elektronische Signatur der Software, die auf dem Gerät installiert werden soll. Wenn eine Kontrolle fehlschlägt, kann die Software nicht installiert werden. Vor Beginn der Installation muss das Softwarepaket „injiziert“ werden, das heißt, mithilfe des Tools Custom Files in den flüchtigen Speicher des Geräts kopiert werden. Dieses Tool stellt sicher, dass außer den geschützten ausführbaren Formaten nur Originaldateien, die von Miltenyi Biotec signiert sind, zur Ausführung auf das Gerät kopiert werden können.

Die Installation einer neuen Version der Gerätesoftware wird unten in Abschnitt 4.1.6 ´Ebene des Update-Handlings´ beschrieben.

Neue Versionen der Gerätesoftware oder kundenspezifische Applikationssoftware werden vom Miltenyi Biotec Technical Support installiert.

Eine spezielle Software zur Erkennung von Schadprogrammen läuft nicht auf dem System, da diese für dieses Produkt nicht geeignet ist. Stattdessen wird das Schadsoftware-Risiko über das Defense-in-Depth-Konzept kontrolliert.

Applikationssoftware und Tools validieren die Benutzereingaben auf Plausibilität. Diese Validierung umfasst unter anderem eine Bereichsvalidierung für numerische Eingaben, eine Validierung der LOT- und Produktnummern von Verbrauchsmaterialien sowie Plausibilitätsprüfungen für Eingaben.

Die Software und Applikationen fordern während des Betriebs nicht zur Eingabe von personenbezogenen Gesundheitsdaten auf. Es besteht ein geringes Risiko,

dass diese während des Anwendungslaufs vom Anwender eingegeben werden. Es liegt in der Verantwortung des Anwenders, sicherzustellen, dass die geltenden Datenschutzvorschriften eingehalten werden.

Protokolle und Log-Daten können aus dem Gerät exportiert werden. Mit den exportierten Dateien werden Datei-Hashes exportiert, damit der Anwender überprüfen kann, ob der Export und die Übertragung an ein nachgelagertes System erfolgreich waren und keine übertragungsbedingte Datenbeschädigung auftrat. Derzeit wird der MD5-Algorithmus verwendet.

Der Zugriff auf Software, die für Wartungszwecke bestimmt ist, und auf zugriffsbeschränkte Funktionalität von Anwendungsverfahren ist nur für den Miltenyi Biotec Technical Support möglich und im Normalbetrieb für den Kunden nicht verfügbar. Zugriff erhalten Benutzer, die sich mit dem Service-Konto oder mit einem Service-USB-Stick, d. h. einem USB-Stick mit Authentifizierungsdaten, und zugehöriger PIN oder über die Fernzugriffsfunktion des Info-Tools in Verbindung mit einer von Miltenyi Biotec bereitgestellten einmaligen PIN anmelden. Nur der Miltenyi Biotec Technical Support erhält die Zugangsdaten für das Service-Konto und den Service-USB-Stick. Eine einmalige PIN kann vom Technischen Support zur Verwendung bei Fällen von Fern-Support bereitgestellt werden.

WICHTIG

Es ist kein Schutzmechanismus eingerichtet, um die exportierten Daten davor zu schützen, gelesen oder absichtlich manipuliert zu werden. Der Kunde muss sicherstellen, dass nur berechtigte Personen Zugriff auf die exportierten Daten erhalten.

4.1.4 Benutzerebene

Jeglicher Zugang zu den Systemkomponenten kann über eine konfigurierbare Benutzerverwaltung geschützt werden. Der Kunde muss sicherstellen, dass die in diesem Dokument enthaltenen Anweisungen und Empfehlungen umgesetzt werden. Darüber hinaus muss der Kunde sicherstellen, dass nur geschultes und autorisiertes Personal Zugang zum Gerät erhält und dass die üblichen bewährten Verfahren bezüglich der Verwendung von Passwörtern sowie die geltenden Vorschriften eingehalten werden.

4.1.5 Audit-Trail-Ebene

Das Audit-Trail-System protokolliert Informationen über die auf dem Gerät durchgeführten Aktionen, z. B. Eingaben des Anwenders während eines Anwendungslaufs oder Veränderungen der Konfiguration des Geräts. Wenn Audit-Trail aktiviert ist, werden alle Aktionen im Audit-Trail des Geräts protokolliert. Der Kunde muss sicherstellen, dass die in diesem Dokument enthaltenen Anweisungen und Empfehlungen befolgt werden. Auch wenn Audit-Trail-Daten

vom Gerät erzeugt werden, bleibt der unsachgemäße Umgang mit Audit-Trail-Daten ein Restrisiko. Um dieses Risiko zu minimieren, ist der Kunde für die Sicherheit und den Umgang mit Audit-Trail-Daten (z. B. Export, Speicherung, Löschung und Überprüfung) gemäß den geltenden Vorschriften verantwortlich.

4.1.6 Ebene des Update-Handlings

Sicherheitsupdates werden im Rahmen von Update-Paketen bereitgestellt. Miltenyi Biotec wird den Kunden informieren, sobald eine neue Software verfügbar ist.

Aktualisierungen der Gerätesoftware dürfen nur vom Miltenyi Biotec Technical Support durchgeführt werden. Die Updates der Gerätesoftware werden entsprechend den Verfahren, die in SOPs von Miltenyi Biotec beschrieben sind, geliefert und installiert. Die Updates kommen in speziellen Paketen, die sowohl die neue Gerätesoftware als auch die Software zur Durchführung der eigentlichen Installation enthalten. Updates werden über einen USB-Stick bereitgestellt. Um die Integrität des Pakets sicherzustellen, sind alle Komponenten kryptografisch signiert, und diese Signatur wird vor der Installation überprüft. Wenden Sie sich für die Planung eines Geräte-Updates an den Miltenyi Biotec Technical Support.

4.1.7 Ebene des Handlings von Sicherheitslücken

Um eine Sicherheitslücke oder ein Vorkommnis betreffend des Produkts oder einer seiner Komponenten zu melden, wenden Sie sich an den Miltenyi Biotec Technical Support (siehe Kapitel 11 ´Fehlerbehebung´).

4.1.8 Ebene der Datensicherung und Wiederherstellung

Das Gerät verfügt nur über die Funktion zur Sicherung von Protokollen und Daten. Der Kunde muss sicherstellen, dass regelmäßig ein Backup dieser Daten gemäß den geltenden Vorschriften durchgeführt wird. Falls die Gerätesoftware nicht mehr funktioniert, kontaktieren Sie den Miltenyi Biotec Technical Support.

4.1.9 Zusammenfassung der sicheren Konfiguration

In den vorstehenden Abschnitten wurden die eingerichteten Sicherheitsmaßnahmen vorgestellt und weitere Maßnahmen für den sicheren Betrieb des CliniMACS Prodigy empfohlen. Diese Maßnahmen betreffen die Bereiche der Konfiguration des Geräts sowie der Verfahren und Richtlinien zur Steigerung der Sicherheit des Geräts. Die folgenden Maßnahmen werden empfohlen:

- Stellen Sie sicher, dass nur autorisierte Personen physischen Zugang zum Gerät und seinen physischen Schnittstellen erhalten.
- Stellen Sie sicher, dass der Zugang zum Netzwerk, in dem das Gerät betrieben wird, auf autorisierte Personen und Systeme beschränkt ist.
- Aktivieren Sie die Authentifizierung und Autorisierung an jedem Gerät, um sicherzustellen, dass nur autorisierte Personen Zugang zur Gerätesoftware haben.
- Der Kunde muss ein entsprechendes Autorisierungsmanagement eingerichtet haben, um sicherzustellen, dass Personen, die das Gerät verwenden oder Zugang dazu haben, nur die Rechte zugewiesen werden, die sie zur Durchführung ihrer Arbeitsaufgabe benötigen (nach dem Least-Privilege-Prinzip).
- Legen Sie geeignete Passwortrichtlinien fest, um bewährte Verfahren und geltende Vorschriften einzuhalten.
- Sichere Protokolle sollten unsicheren Varianten vorgezogen werden, wenn das Gerät Erstere unterstützt.
- Aufgrund der fehlenden Verschlüsselung des FTP-Datenverkehrs zum und vom Gerät wird empfohlen, eigens ein Benutzerkonto für den Zugriff auf Daten via FTP einzurichten und zu verwenden.
- Es müssen Prozesse und Verfahren eingerichtet werden, die sicherstellen, dass nur zulässige und kontrollierte USB-Sticks verwendet werden und die Verwendung anderer USB-Sticks verhindert wird.
- Es müssen Prozesse und Verfahren eingerichtet sein, um den adäquaten Umgang mit Audit-Trails, Protokollen und Log-Daten gemäß den geltenden Vorschriften sicherzustellen.
- Das Personal muss in Bezug auf Sicherheitsbewusstsein und grundlegende Sicherheitshygiene geschult sein.
- Prozesse und Verfahren müssen sicherstellen, dass regelmäßig Backups des Geräts gemäß den geltenden Vorschriften durchgeführt werden.
- Es liegt in der Verantwortung des Kunden, dafür zu sorgen, dass keine personenbezogenen Gesundheitsdaten im Gerät verwendet werden.

5

Softwarekonzept

5.1 Grundkonzept

Die Software, die auf dem Gerät läuft, besteht aus der Kernsoftware und verschiedener Anwendungssoftware (sogenannte Anwendungsprozesse). Die Kernsoftware ist die gemeinsame Plattform für alle ausführbaren Programme, einschließlich der Anwendungsprozesse, Tools und Einstellungen.

Anwendungsprozess

Eine jeweils eigenständige Software steht für einen biologischen Prozess, wie z. B. den T Cell Transduction Process oder das LP-34 Enrichment. Sie steuert eine Sequenz von vordefinierten Hardware- und Softwareschritten zur Automatisierung des biologischen Prozesses. Der Anwender wird Schritt für Schritt durch den Prozess geführt. Es gibt zwei Arten von Anwendungsprozessen:

- Standardanwendungsprozess: Ein validierter Anwendungsprozess, der standardmäßig zur Verfügung gestellt wird.
- Kundenspezifischer Anwendungsprozess (CAP): Ein maßgeschneiderter Anwendungsprozess, der für bestimmte Kunden entwickelt wurde.

Werkzeug

Ein ausführbares Programm, das eine universelle Funktion außerhalb eines Anwendungsprozesses durchführen kann. Zum Beispiel die Überprüfung oder Änderung des Status der Hardware, die Datenübertragung oder das Herunterfahren des Geräts.

Einstellungen

Ein ausführbares Programm zur Konfiguration des Geräts. Zum Beispiel Network Settings (Netzwerkeinstellungen), Customer Settings (benutzerdefinierte Einstellungen) und Module Settings (Einstellungen für die Module).

Für jedes ausführbare Programm wird ein Ordner erstellt, der alle Informationen enthält. Der Ordner wird nach
[Datum] _ [Uhrzeit] _ [Seriennummer] _ [ausführbares Programm] benannt.

Der Inhalt dieses Ordners wird durch das ausgeführte Programm gesteuert. Die kundenrelevanten Dateien für Anwendungsprozesse sind in Tabelle 5.1 aufgeführt

Datei-/ Ordnername	Beschreibung	Format
Protocol.pdf	Elektronische Aufzeichnung des Anwendungablaufs	.pdf
Prototol_ Appendix_I.pdf	Fehler- und Warnprotokoll während der Ausführung der Anwendung	.pdf
Interphase	Kamerabilder von Zwischenschichten	Ordner
Microscope	Mikroskopbilder, die während der Anwendung aufgenommen wurden	Ordner
checksums.md5	Prüfsumme	.md5
IR_Monitor	Protokolliert die Zeit und Temperatur, wenn die Oberflächentemperatur der Kammer während der Zellkultivierung außerhalb der Spezifikation liegt	.html

Tabelle 5.1: Protokolldateien von Anwendungsprozessen

5.2 Grafische Benutzeroberfläche

Die grafische Benutzeroberfläche besteht aus verschiedenen Bereichen: Menüleiste (mit Schnellzugriffsmenü), Werkzeugleiste, Statuszeile und Inhaltsbereich (Abbildung 5.1). Während des Betriebs der Software verändern sich die angezeigten Elemente und Inhalte entsprechend den jeweiligen Aktivitäten und Prozessen.

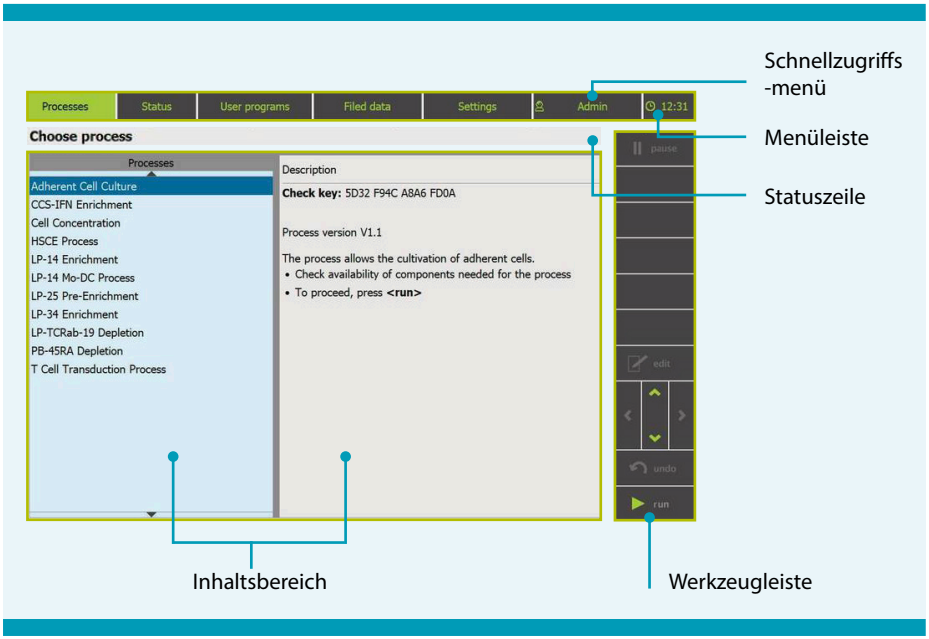


Abbildung 5.1: Bereiche der grafischen Benutzeroberfläche

5.2.1 Menüleiste und Inhaltsbereich

Die Menüleiste ermöglicht den Zugriff auf die Menüs **<Processes>** (Prozesse), **<Status>** (Status), **<User Programs>** (Benutzerprogramme), **<Filed data>** (Daten), **<Settings>** (Einstellungen) und (quick access menu) (Schnellzugriffsmenü). Das aktive Menü wird grün unterlegt angezeigt. Auf den jeweiligen Bereich drücken, um das Menü zu aktivieren. Der Inhaltsbereich passt sich dem ausgewählten Menü an. Nach der Anmeldung ist standardmäßig **< Processes >** ausgewählt und der Inhalt für Prozesse wird angezeigt (siehe Abbildung 5.1).

Menü	Beschreibung
<Processes> (Prozesse)	Ermöglicht den Zugriff auf die Standard-Anwendungsprozesse, die auf dem Gerät installiert sind (Bildschirm 6.5) und führt den Anwender durch den Prozesslauf (Bildschirm 6.6)
<Status> (Status)	Zeigt den Gerätestatus während eines laufenden Anwendungsprozesses an (Abbildung 6.1)
<User Programs> (Benutzerprogramme)	Ermöglicht den Zugriff auf den Miltenyi Biotec Customized Application Process (CAP) und führt durch den Prozesslauf
<Filed data> (Daten)	Ermöglicht das Anzeigen und Exportieren der von Prozessen, Tools und Einstellungen erzeugten Daten (Bildschirm 7.1).
<Settings> (Einstellungen)	Erlaubt den Zugriff auf Einstellungen und Tools für die Gerätekonfiguration, Funktionstests und Fehlerbehebung (Bildschirm 8.1)
Quick access menu (Schnellzugriffsmenü)	Ermöglicht den Zugriff auf Logout, Benutzermanagement, Passwortrichtlinien, Audit-Trail und die Schaltfläche Shutdown (Bildschirm 6.3)
System time (Systemzeit)	Zeigt die aktuelle Systemzeit an.

Tabelle 5.2: Menüs in der Menüleiste

5.2.2 Statuszeile

Die Statuszeile (siehe Abbildung 5.1) enthält kurze Informationen zum Status des laufenden Prozesses.

5.2.3 Werkzeugleiste

Die Werkzeugleiste enthält verschiedene Schaltflächen zur Steuerung des Prozesses. Welche der Schaltflächen verfügbar und aktiv sind, hängt vom jeweiligen Anwendungsprozess ab. Abbildung 5.2 zeigt Beispiele für die Werkzeugleisten im Verlauf von zwei verschiedenen Anwendungsprozessen. Die grüne Farbe zeigt an, dass die Schaltfläche 'aktiv' ist, und die graue Farbe, dass die Schaltfläche 'inaktiv' ist. Häufig verwendete Schaltflächen werden erklärt in Tabelle 5.3.

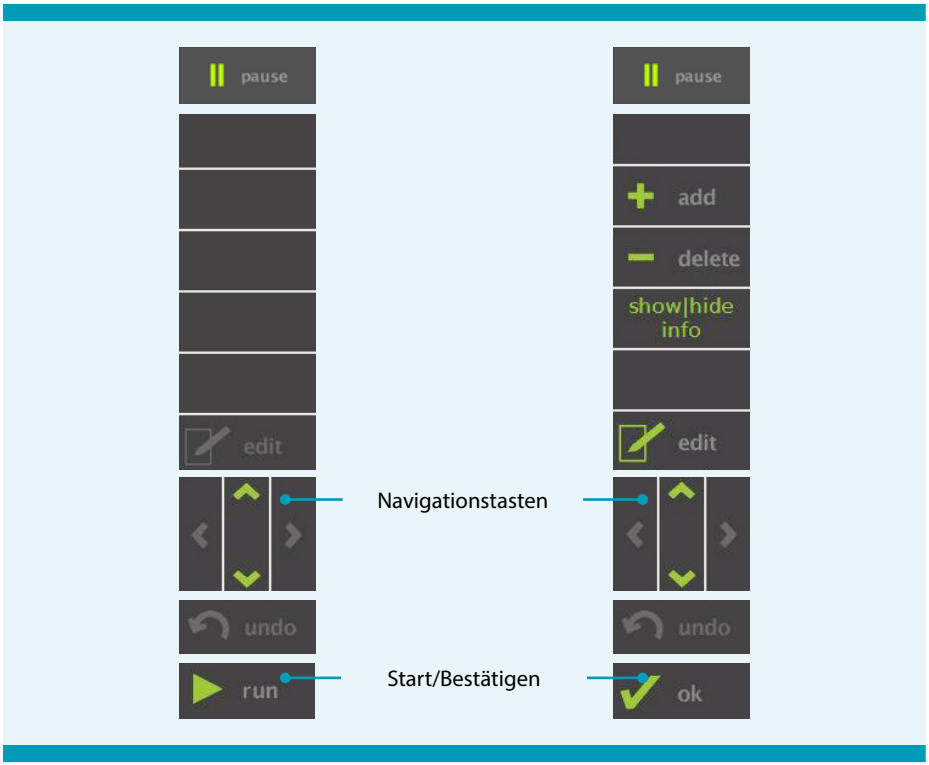


Abbildung 5.2: Dynamische und statische Schaltflächen in der Werkzeugleiste

Name der Schaltfläche	Beschreibung	Verfügbarkeit
<pause>	vorübergehendes Anhalten/Unterbrechen des laufenden Prozesses, hängt von der laufenden Anwendung ab	während eines Prozesslaufs
<edit>	aktiviert das Tastenfeld für die manuelle Dateneingabe (siehe 5.2.4 ´Eingabefelder´).	wenn Eingabefelder verfügbar sind
Navigations-tasten	zum Wählen von Elementen aus einer Liste: mit ^v kann das gewählte Element in der Liste nach oben oder unten verschoben werden (siehe Bildschirm 6.5) oder mit < > kann zwischen Listen gewechselt werden (siehe Bildschirm 8.1). zum Navigieren in Bildern der Kamera (Abbildung 6.3).	immer wenn die Kamera aktiv ist
<undo>	macht eine oder mehrere Eingaben rückgängig und stellt den ursprünglichen Inhalt des Bildschirms wieder her	während eines Prozesslaufs
<ok>/<run>	<ok> bestätigt eine Auswahl oder schließt das aktive Menü <run> startet einen Prozess, ein Benutzerprogramm oder ein sonstiges Verfahren	immer

Tabelle 5.3: Häufig verwendete Schaltflächen der Werkzeugleiste

5.2.4 Eingabefelder

Ein Eingabefeld stellt eine Tastatur dar und ermöglicht die Eingabe von Buchstaben oder Ziffern (siehe Abbildung 5.3). Zur manuellen Eingabe von Großbuchstaben auf <⇧> drücken, für ein Leerzeichen auf <SP> drücken, für Ziffern auf <?123> drücken, und zur Verwendung der Rücktaste auf <⌫> drücken. Zum Öffnen von Eingabefeldern in der Werkzeugleiste auf <edit> (Bearbeiten) drücken. Zum Schließen eines Eingabefeldes entweder auf <ok> unten rechts drücken, um die Eingabe zu bestätigen, oder auf <Schließen> oben rechts, um das Eingabefeld zu schließen, ohne die Eingabe zu speichern.

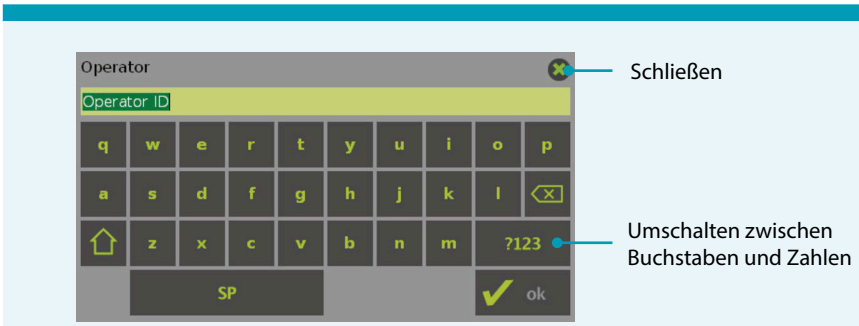
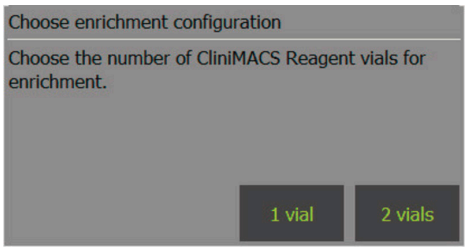


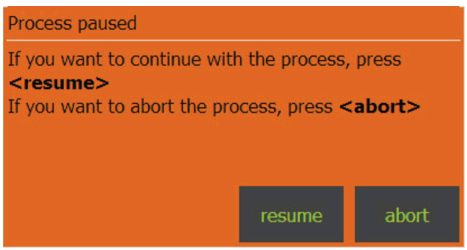
Abbildung 5.3: Eingabefeld - Tastatur mit Buchstaben

5.2.5 Pop-up-Fenster

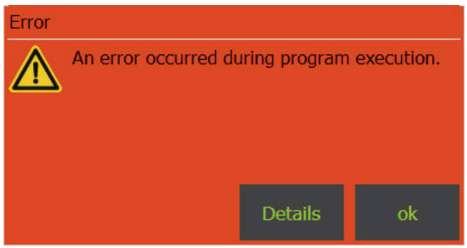
Pop-up-Fenster können angezeigt werden, während ausführbare Programme laufen. Der laufende Prozess wird unterbrochen, bis das Pop-up-Fenster geschlossen wird. Falls erforderlich, können die Pop-up-Fenster durch Anklicken der Leiste am oberen Rand an beliebige Stellen auf dem Bildschirm versetzt werden. Ein Pop-up-Fenster kann in verschiedenen Szenarien angezeigt werden:



Eine Eingabe oder eine Bestätigung ist erforderlich. Das Pop-up-Fenster hat einen grauen Hintergrund. Eine der Schaltflächen wählen, um mit dem Prozess fortzufahren.



Warnung des Geräts, oder eine wichtige Entscheidung muss bestätigt werden. Das Pop-up-Fenster hat einen orangefarbenen Hintergrund. Eine der Schaltflächen wählen, um eine Entscheidung zu treffen.



Ein Fehler ist aufgetreten. Das Pop-up-Fenster hat einen roten Hintergrund. Eine der Schaltflächen am unteren Rand wählen, um fortzufahren.

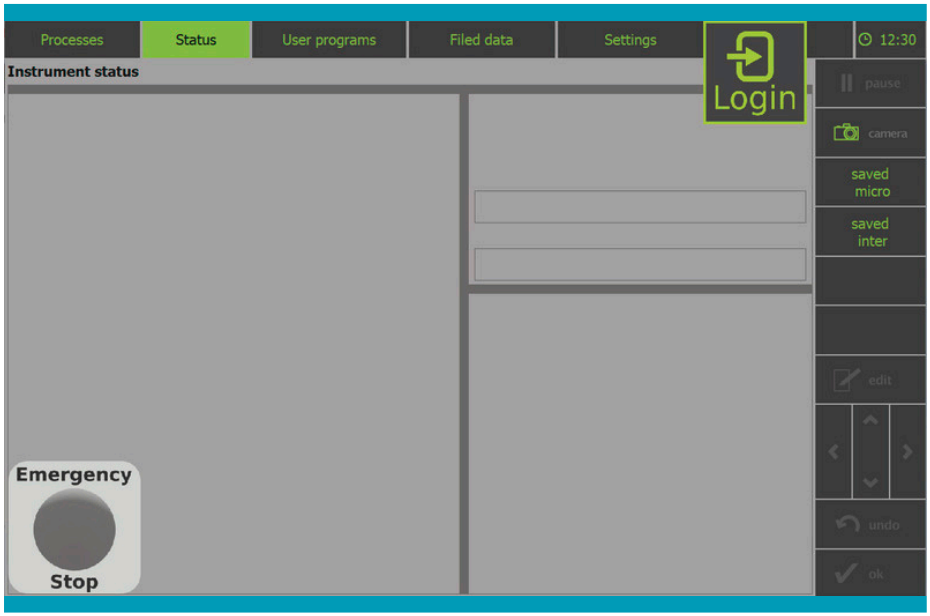
Bei Bedarf den Miltenyi Biotec Technical Support kontaktieren.

6

Grundlegender Betrieb

6.1 Einschalten des Geräts

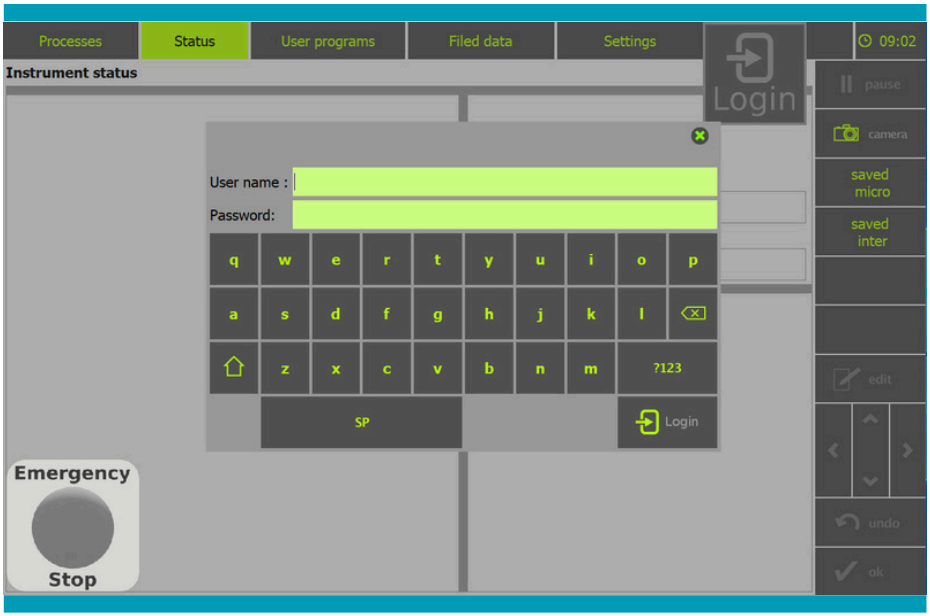
Den CliniMACS Prodigy mit dem Netzschalter an der Rückseite des Geräts einschalten. Der Startbildschirm zeigt die Softwareversion an, und der Initialisierungsprozess erscheint kurz (ca. 5 Sekunden). Nach dem Initialisierungsprozess erscheint ein gesperrter Bildschirm (siehe Bildschirm 6.1). Auf diesem Bildschirm ist nur die Schaltfläche **<Login>** aktiv.



Bildschirm 6.1: Gesperrter Bildschirm

6.2 Login

Auf <Login> (Anmelden) in der rechten oberen Ecke des Bildschirms drücken, um das Pop-up-Fenster <User Login> zu öffnen (siehe Bildschirm 6.2). Den Benutzernamen und das Passwort eingeben und auf <Login> drücken. Der Bildschirm wird entsperrt. Benutzername und Passwort müssen vor der Verwendung des Geräts eingerichtet werden (siehe Kapitel 10 ´Benutzerverwaltung´ für Einzelheiten).



Bildschirm 6.2: Login-Fenster

Anmerkung: Falls das Login fehlschlägt, kontaktieren Sie einen Systemadministrator, um Folgendes zu verifizieren:

- Korrektheit von Benutzername und Passwort.
- Zugriffsrechte für dieses Konto. Weitere Informationen siehe Kapitel 10 ´Benutzerverwaltung´.

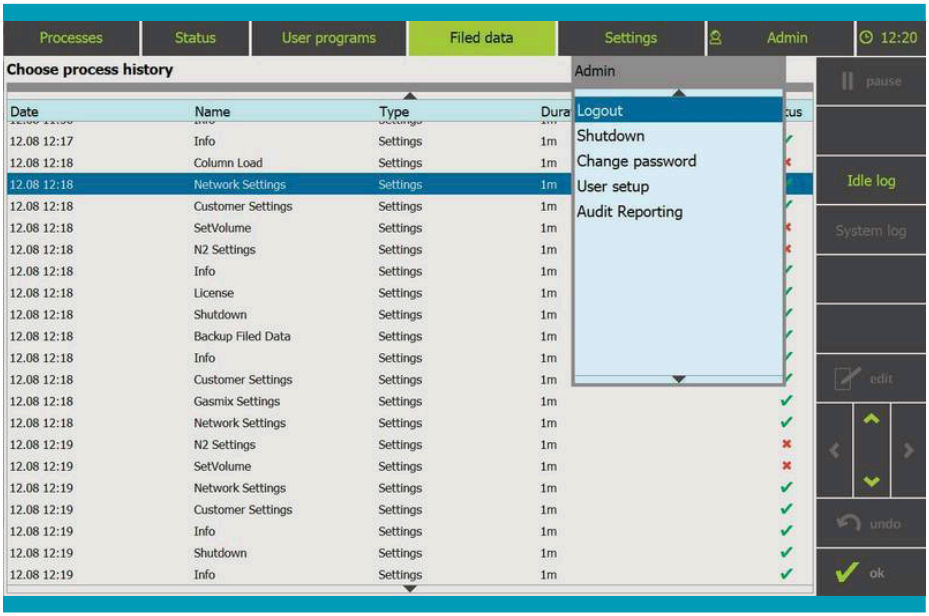
Wenn während der Anmeldung eine Popup-Benachrichtigung angezeigt wird, die nicht mit falschen Benutzerdaten oder fehlenden Zugriffsrechten zusammenhängt, auf <OK> drücken. Dann erneut die Anmeldedaten des Benutzers eingeben.

Falls das Login weiterhin fehlschlägt, wenden Sie sich an den Miltenyi Biotec Technical Support.

6.3 Logout (Abmelden)

Auf (Schnellzugriffsmenü) drücken und <Logout> aus der Liste auswählen (siehe Bildschirm 6.3). Der Bildschirm wird wieder gesperrt.

Anmerkung: Erfolgt für 20 Minuten keine Interaktion mit der Software, wird der Benutzer automatisch abgemeldet.



Bildschirm 6.3: Logout (Abmelden)

6.4 Abschalten

Auf (Schnellzugriffsmenü) drücken. <Shutdown> aus der Liste auswählen (siehe Bildschirm 6.3). Alternativ gehen Sie zu <Settings> ▸ <Tools> ▸ <Shutdown>. Warten, bis der Shutdown-Prozess beendet ist, und dann das Gerät mit dem Netzschalter an der Rückseite ausschalten.

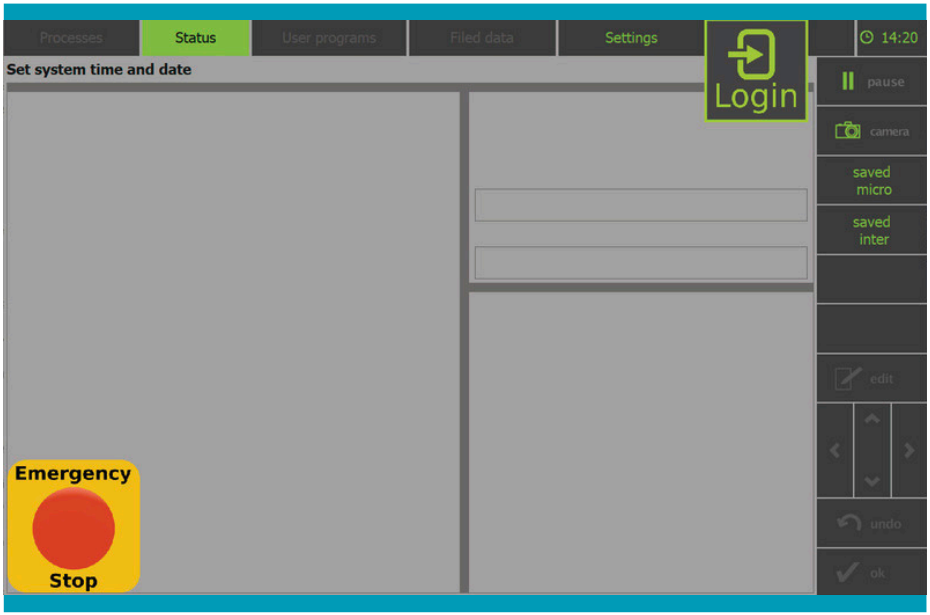
6.5 Not-Aus-Funktion

Die Schaltfläche <Emergency Stop> (Not-Aus-Funktion) hält die laufende Anwendung oder ein Tool in einer Notsituation an, ohne dass zuvor ein Login durchgeführt werden muss. Um die Anforderungen von 21 CFR Part 11 zu erfüllen, ist ein nachfolgendes Login mit Angabe der Begründung für die Not-Aus-Schaltung erforderlich. Die Not-Aus-Schaltung über die <Emergency Stop> Schaltfläche wird nur dann aktiviert (angezeigt durch die Farben gelb und rot), wenn eine Anwendung oder ein Tool aktiv ist und kein Benutzer angemeldet ist (siehe Bildschirm 6.4).

WICHTIG

Die Notausschaltung <Emergency Stop> schaltet das Gerät nicht vollständig aus, sondern hat dieselbe Funktion wie die Schaltfläche <pause> während einer aktiven Anwendung, wenn der Benutzer angemeldet ist.

Um die Anwendung fortzusetzen, muss sich ein Benutzer mit der entsprechenden Berechtigung für die Anwendung anmelden.

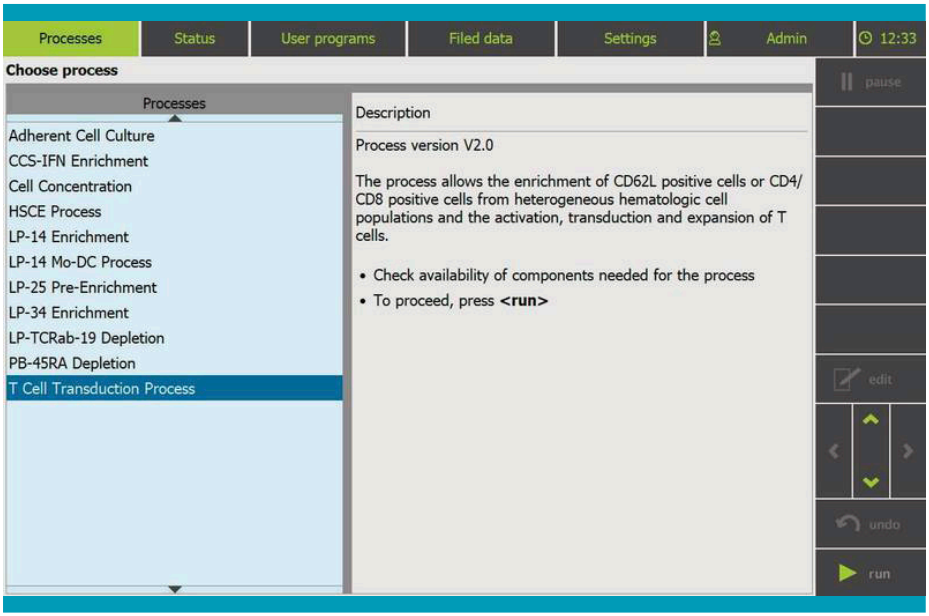


Bildschirm 6.4: Schaltfläche <Emergency Stop>

6.6 Wählen eines Anwendungsprozesses

1. Auf <Prozesse> in der Menüleiste drücken, um einen Standard-Anwendungsprozess auszuwählen. Zum Auswählen eines CAP auf <Benutzerprogramme> drücken.
2. Den gewünschten Prozess aus der Prozessliste auswählen (Bildschirm 6.5). Der gewählte Prozess wird blau hinterlegt. Eine Beschreibung der Anwendung wird rechts angezeigt. In die Prozessliste drücken oder mit ^ und ⌄ in der Werkzeugleiste durch die verfügbaren Prozesse navigieren.

Anmerkung: Der Inhalt der Prozessliste entspricht der Rolle und den Rechten des aktuell angemeldeten Benutzers. Es werden nur die Anwendungen angezeigt, für die der aktuell angemeldete Benutzer Zugriffsrechte hat. Weitere Informationen zu Rollen und Rechten siehe Kapitel 10 ´Benutzerverwaltung´.



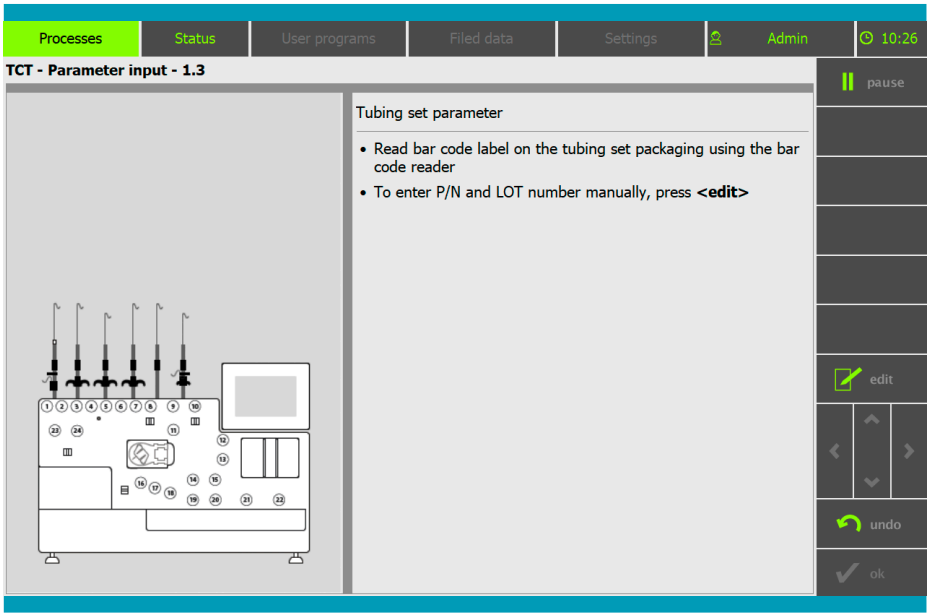
Bildschirm 6.5: Wählen eines Anwendungsprozesses

6.7 Ausführen eines Anwendungsprozesses

Zum Starten eines ausgewählten Prozesses in der Werkzeugleiste auf **<run>** drücken. Die Software führt den Anwender Schritt für Schritt durch den Prozess. Bildschirm 6.6 zeigt als Beispiel einen Schritt der TCT-Anwendung. In der Statuszeile wird der aktuelle Schrittname mit Nummerierung angezeigt. Im Inhaltsbereich erscheinen weitere Informationen zum betreffenden Prozessschritt. Beachten Sie die Abbildung und die Anweisungen im Inhaltsbereich zu jedem Schritt.

Bei einigen Prozessschritten sind Benutzereingaben erforderlich. Typische erforderliche Eingaben sind Materialnummer (P/N), LOT-Nummer und Messwerte. Die Materialnummer und LOT-Nummer können entweder mit dem Barcode-Lesegerät oder manuell eingegeben werden. Zur manuellen Eingabe, oder wenn die Eingabe mit dem Barcode-Lesegerät nicht angenommen wird, in der Werkzeugleiste auf **<edit>** drücken und das Eingabefeld verwenden.

Wenn alle erforderlichen Aktionen abgeschlossen sind, wird **<ok>** in der Werkzeugleiste aktiviert. Um zum nächsten Schritt zu gelangen, **<ok>** drücken. Um zum vorherigen Schritt zu gelangen, **<undo>** (**<Rückgängig>**) drücken.



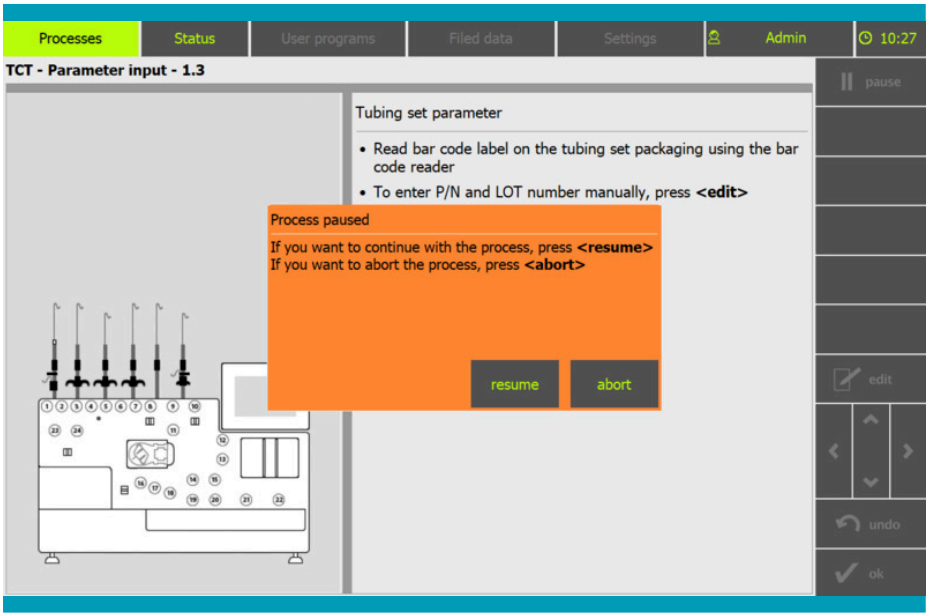
Bildschirm 6.6: Beispiel eines Schrittes im TCT-Anwendungsprozess

6.8 Anhalten eines Anwendungsprozesses

Um einen laufenden Prozess anzuhalten, <pause> in der Werkzeugleiste drücken. Es erscheint ein Pop-up-Fenster (Bildschirm 6.7). Um einen angehaltenen Prozess fortzusetzen, auf <resume> drücken. Um den Prozess zu beenden, <abort> drücken.

WICHTIG

Ein abgebrochener Prozess kann nicht fortgesetzt werden.



Bildschirm 6.7: Prozess angehalten

6.9 Gerätestatus und Status des Anwendungsprozesses

Um den Betriebsstatus des laufenden Prozesses zu überprüfen, auf <Status> in der Menüleiste drücken. Der Inhaltsbereich zeigt folgende Elemente an:

- Prozessbezogene Parameter: eine Liste aller relevanten Prozessparameter (siehe Abbildung 6.1, links).
- Infofeld und Fortschrittsbalken:
  Prozessinformationen (siehe Abbildung 6.1, oben rechts):
  - Anwendername
  - Probeninformation
  - Fortschritt des Teilprozesses und Restzeit
  - Fortschritt des Prozesses und Restzeit bis zur nächsten Benutzerinteraktion
- Prozessgrafik: zeigt den Status des laufenden Teilprozesses grafisch an (siehe Abbildung 6.1, unten links). Alle aktiven Komponenten des Geräts (z. B. Schlauchpumpe, Quetschventile) sind orange dargestellt.

Anmerkung: Die Statusinformationen werden nur während einer laufenden Applikation angezeigt. Diese Bildschirmseite ist leer, wenn keine Anwendung läuft.

Die Prozessgrafik ist bei CAPs unter Umständen nicht verfügbar.

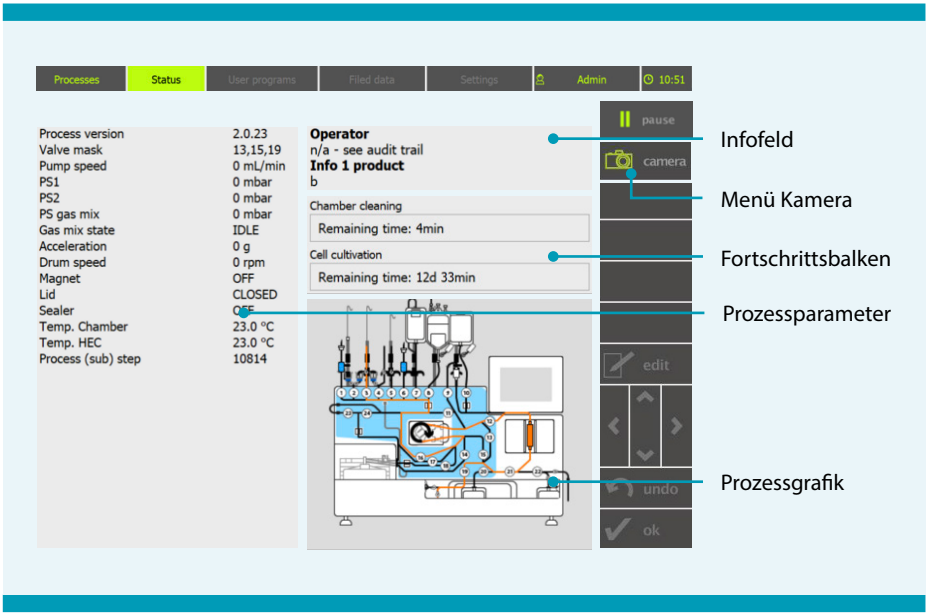


Abbildung 6.1: Übersicht über den Status des Geräts

6.10 Aufnehmen von Bildern

Während ausgewählter Anwendungen können zwei Kamerafunktionen mit <camera> in der Werkzeugleiste verwendet werden (siehe Abbildung 6.1).

- Aufnahme der Layer Detection Camera: Dieses Bild wird verwendet, um die Volumina von Zentrifugationsfraktionen zu messen. Es ist nur in ausgewählten Applikationen und während der ersten Volumeneinstellung nach dem Laden der Probe verfügbar (siehe Abbildung 6.2).
- Mikroskopaufnahme: Dieses Bild kann verwendet werden, um eine Zellkultur visuell zu überwachen. Es ist nur im Verlauf von Zellkulturverfahren verfügbar (siehe Abbildung 6.3).

Das Bild wird vom Anwendungsprozess automatisch erfasst und im Protokoll gespeichert. Um Bilder anzuzeigen, auf <camera> in der Werkzeugleiste drücken, wenn das Menü <Status> ausgewählt ist (siehe Abbildung 6.1). Entsprechend dem Schritt des Anwendungsprozesses wird im Inhaltsbereich entweder ein Bild der Layer Detection Camera oder ein Mikroskopbild angezeigt.

Anmerkung: Ob das Tool <camera> in der Werkzeugleiste verfügbar ist, hängt von der Art des Anwendungsprozesses ab. Die Bilder werden während der laufenden Anwendung automatisch aufgezeichnet.

6.10.1 Layer Detection Camera

Die verschiedenen Schichten werden automatisch von der Software detektiert. In Abbildung 6.2 kennzeichnen rote und orangefarbene Striche die Position der Schichten im Bild. Das Diagramm darunter zeigt die aufgezeichneten Volumina der Zentrifugationsfraktionen. Die Kurven werden, entsprechend zu den Strichen im Bild, in rot und orange dargestellt (siehe Abbildung 6.2).



Abbildung 6.2: Übersicht über den Status des Geräts

Die folgenden Funktionen werden unterstützt:

- Bildaufzeichnung: Auf <snap> in der Werkzeugleiste drücken. Nach einer kurzen Aufzeichnungsphase (ca. 15 Sekunden) wird das angezeigte Bild durch das neu aufgezeichnete Bild ersetzt.
- Bildarchivierung: Auf <save> in der Werkzeugleiste drücken. Das aufgezeichnete Bild wird in das Protokoll des laufenden Prozesses eingebunden.
- Schließen des Kamera-Menüs: Auf <ok> in der Werkzeugleiste drücken.

Anmerkung: Ob die oben angegebenen Schaltflächen in der Werkzeugleiste verfügbar sind, hängt von der Art des Anwendungsprozesses ab.

6.10.2 Mikroskopkamera

Das Menü Kamera zeigt das zuletzt von der integrierten Mikroskopkamera gespeicherte Bild (siehe Abbildung 6.3).

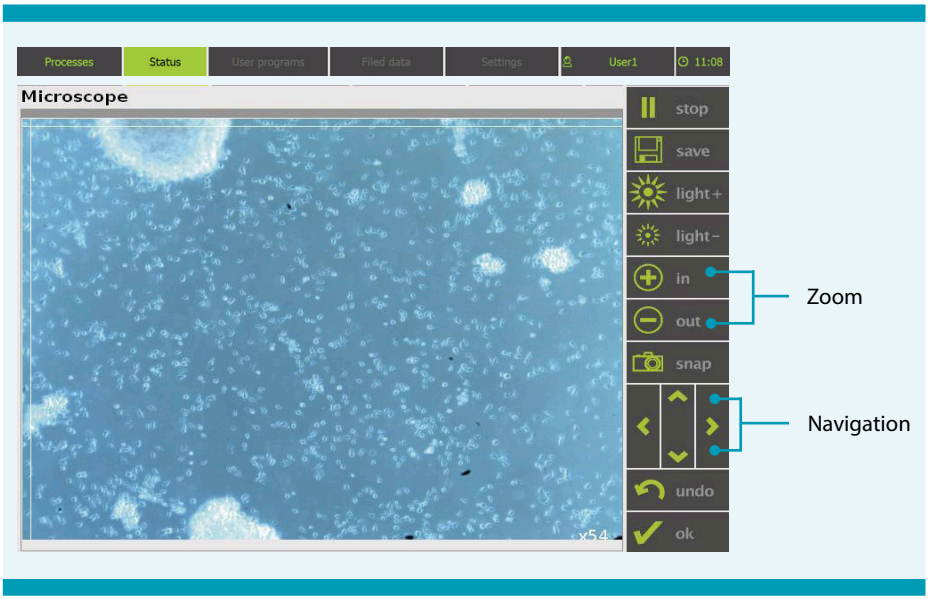


Abbildung 6.3: Statusbildschirm bei aktiver Mikroskopkamera

Die folgenden Funktionen werden unterstützt:

- Bild vergrößern: Bei Berühren eines Punkts im Bild der Mikroskopkamera wird das Bild 2-fach vergrößert. Der berührte Punkt wird in die Bildmitte gerückt. Die Bilder können bis zu 400-fach vergrößert werden.
- Im Bild navigieren: Durch Drücken einer Navigationstaste kann das Bild um ein Halbbild in die gewählte Richtung verschoben werden. Bildlaufleisten zeigen die absolute Position des Bildausschnitts im Gesamtbild und erleichtern so die Navigation. Durch wiederholtes Drücken der Schaltfläche «undo» können die letzten zehn Navigationsschritte einzeln rückgängig gemacht werden.
- Bildaufzeichnung: Auf **<snap>** in der Werkzeugleiste drücken. Nach einer kurzen Aufzeichnungsphase (ca. 15 Sekunden) wird das angezeigte Bild durch das neu aufgezeichnete Bild ersetzt.
- Bildarchivierung: Auf **<save>** in der Werkzeugleiste drücken. Das aufgezeichnete Bild wird in das Protokoll des laufenden Prozesses eingebunden.
- Schließen des Kamera-Menüs: Zum Schließen des Kamera-Menüs auf **<ok>** in der Werkzeugleiste drücken.

Anmerkung: Ob die oben angegebenen Schaltflächen in der Werkzeugleiste verfügbar sind, hängt von der Art des Anwendungsprozesses ab.

7 Datenzugriff

7.1 Abrufen von Anwendungsprotokollen

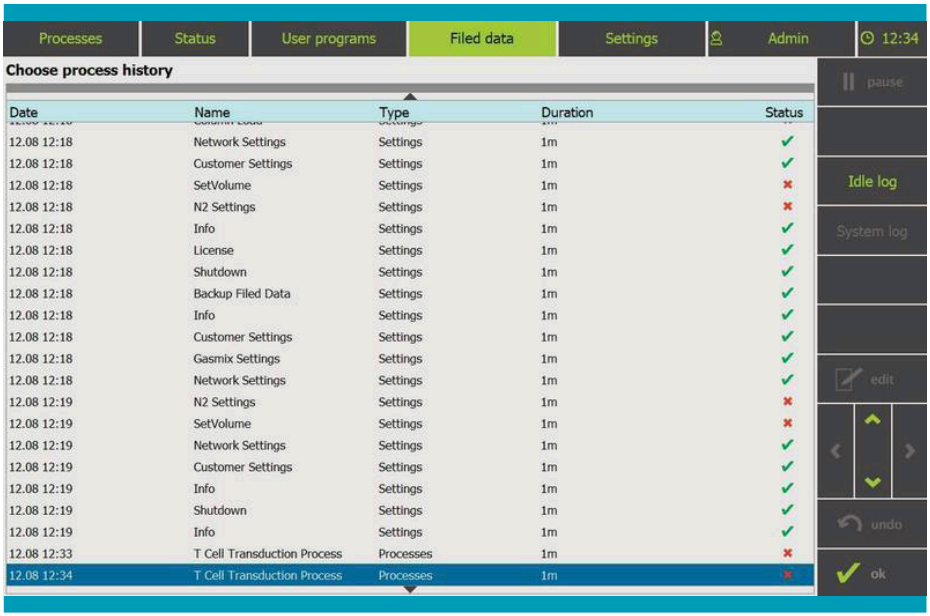
7.1.1 Anzeigen und Exportieren von Protokolldateien auf einen USB-Stick

Das Menü **<Filed data>** (Daten) zeigt die Protokolldateien an, die von Anwendungsprozessen, Tools und Einstellungen erstellt werden. Im Inhaltsbereich wird die Dateiliste mit Datum/Uhrzeit, Name, Typ, Dauer und Status des Prozesslaufs angezeigt (Bildschirm 7.1).

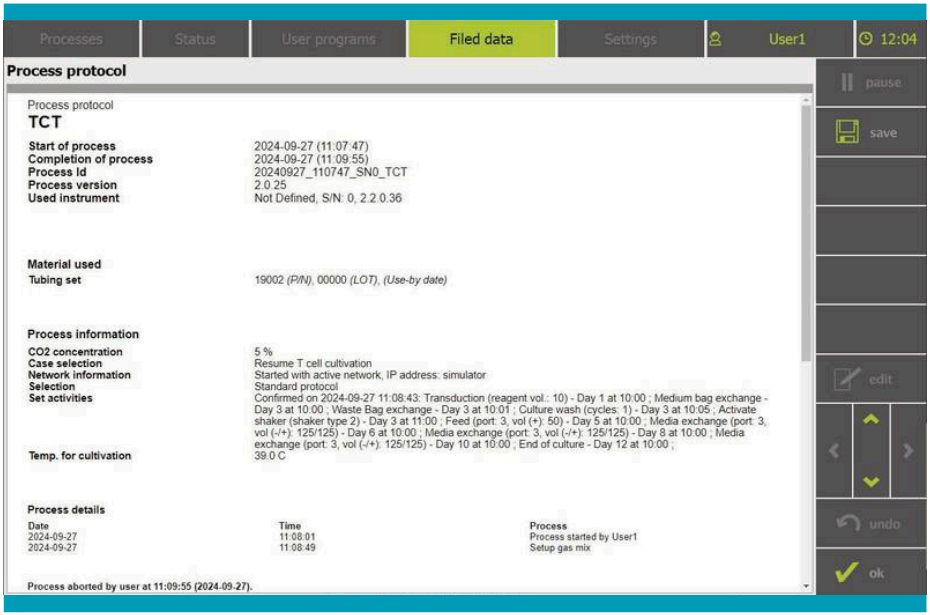
Anmerkung: Das Menü **<Filed data>** ist nicht verfügbar, wenn ein Prozess läuft. Die dazugehörige Schaltfläche ist deaktiviert.

Anzeigen von Protokolldateien

Um den Inhalt der Prozessprotokoll-PDF und der Protokollanhang-PDF anzuzeigen, das gewünschte Protokoll auswählen und **<ok>** drücken (siehe Bildschirm 7.1). Der Inhalt der gewählten Datei erscheint im Inhaltsbereich (siehe Bildschirm 7.2). Erneutes Drücken von **<ok>** führt zur Dateiliste zurück.



Bildschirm 7.1: Beispiel einer Dateiliste



Bildschirm 7.2: Beispiel eines Prozessprotokolls (TCT-Applikation)

Exportieren auf USB-Stick

1. Einen USB-Stick einstecken.
2. Die gewünschte Protokolldatei öffnen und auf <save> in der Werkzeugleiste drücken.

WICHTIG

- Achten Sie darauf, dass der Name des USB-Sticks nicht 'netext' lautet, da dieser Begriff für die Software reserviert ist.
- Zur Sicherung aller Prozessdaten kann das Tool 'Backup Filed Data' (Datensicherung für Dateien) verwendet werden, siehe Abschnitt 8.2.2 ´Backup Filed Data (Datensicherung für Dateien)´.
- Der USB-Stick muss im FAT32-Format formatiert sein und darf nicht passwortgeschützt sein.

7.1.2 Abrufen über FTP

FTP ist ein Netzwerkprotokoll, das die Übertragung von Daten zwischen dem CliniMACS Prodigy (fungiert als FTP-Server) und dem Computer des Endbenutzers (fungiert als FTP-Client) über IP-(Internet-Protocol-)Verbindungen ermöglicht. Alle Protokolldateien, die während des Anwendungslaufs erzeugt werden, können abgerufen werden.

Damit Daten über FTP abgerufen werden können, muss das Gerät entsprechend konfiguriert sein. Um das Gerät für die FTP-Verbindung zu konfigurieren, folgen Sie den Anweisungen in Abschnitt 9.4.1 ´Einrichten des Geräts´. Nach der Konfiguration kann das Gerät mit jedem verfügbaren FTP-Client (z. B. FileZilla) verbunden werden, um Protokolle und Protokolldateien herunterzuladen. Abbildung 7.1 zeigt ein Beispiel für die Verbindungsparameter. Zur Verbindung mit dem Gerät sind folgende Angaben einzugeben:

- Die IP-Addresse des Geräts. Diese findet sich unter **<Settings>** ▸ **<Tools>** ▸ **<Info>** ▸ **<Netzwerk-Information>**.
- Port: Den Standardport 21 verwenden.
- Für Benutzernamen und Passwort werden zwei Anmeldeoptionen unterstützt:
  - Login-Option 1: Ein registriertes Benutzerkonto im Benutzerverwaltungssystem (siehe Kapitel 10 ´Benutzerverwaltung´). In diesem Fall Benutzerkonto und Passwort verwenden. Die Herstellung und Beendigung der Verbindung werden im Audit-Trail aufgezeichnet.
  - Login-Option 2: Ein lokaler Benutzername und Passwort in den FTP/File-Share-Einstellungen. Die Login-Info findet sich unter **<Settings>** ▸ **<Netzwerkeinstellungen>** FTP/FS. In diesem Fall werden die Herstellung und Beendigung der Verbindung nicht im Audit-Trail aufgezeichnet.

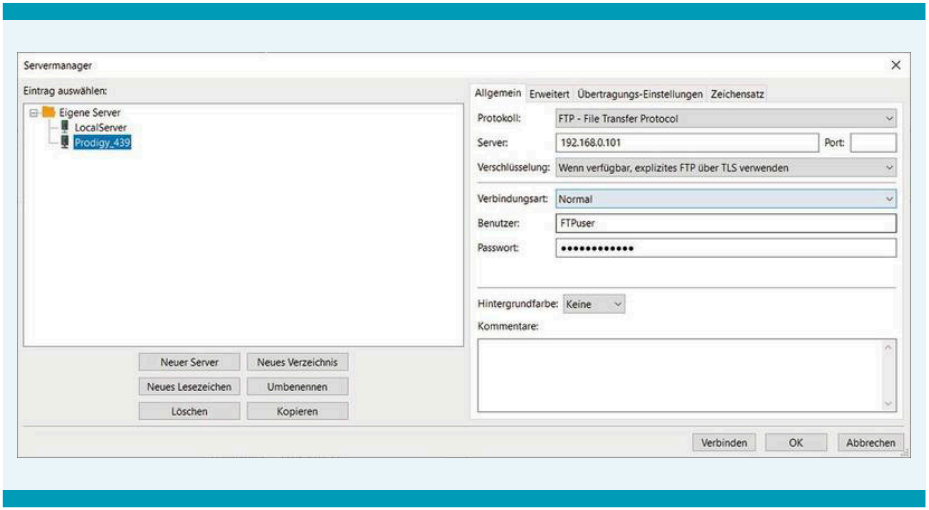


Abbildung 7.1: Beispiel für Verbindungsparameter

WICHTIG

- Wenn Login-Option 1 verwendet wird, ist darauf zu achten, dass die Rolle 'File management user' (Benutzer der Dateiverwaltung) diesem Konto zugewiesen ist. Wie Rollen zu Benutzerkonten zugewiesen werden, wird im Kapitel 10 'Benutzerverwaltung' beschrieben.
- Die Software unterstützt nicht das Protokoll „secured FTP" (sFTP). Es wird empfohlen, das Gerät in einem abgetrennten Netzwerk zu betreiben, wenn über FTP auf Dateien zugegriffen wird.

Anmerkung: Ein einzelner Benutzer kann immer nur eine einzige Verbindung herstellen, da der Server des Geräts keine mehrfachen Verbindungen zulässt. Wenn eine Client-Software verwendet wird, die simultane Verbindungen nutzt (z. B. FileZilla), sind die Einstellungen des Clients entsprechend dahingehend zu ändern, dass jeweils nur eine einzige Sitzung erlaubt ist. Anderenfalls kann der Inhalt nur angesehen, aber nicht heruntergeladen werden.

7.1.3 Abrufen von Dateien über File Sharing

Die während eines Anwendungslaufs erzeugten Protokolldateien können über einen gemeinsam genutzten Netzwerkordner abgerufen werden. Nach Abschluss des Anwendungslaufs werden alle generierten Dateien automatisch in einen Unterordner für jedes Gerät innerhalb des gemeinsam genutzten Ordners platziert. Abbildung 7.2 zeigt die Dateistruktur im gemeinsam genutzten Ordner. Um File Sharing zu ermöglichen, muss das Gerät entsprechend konfiguriert sein. Zur Einrichtung des File Sharings folgen Sie den Anweisungen in Abschnitt 9.3 'Verbindung zu einem Netzlaufwerk herstellen'.

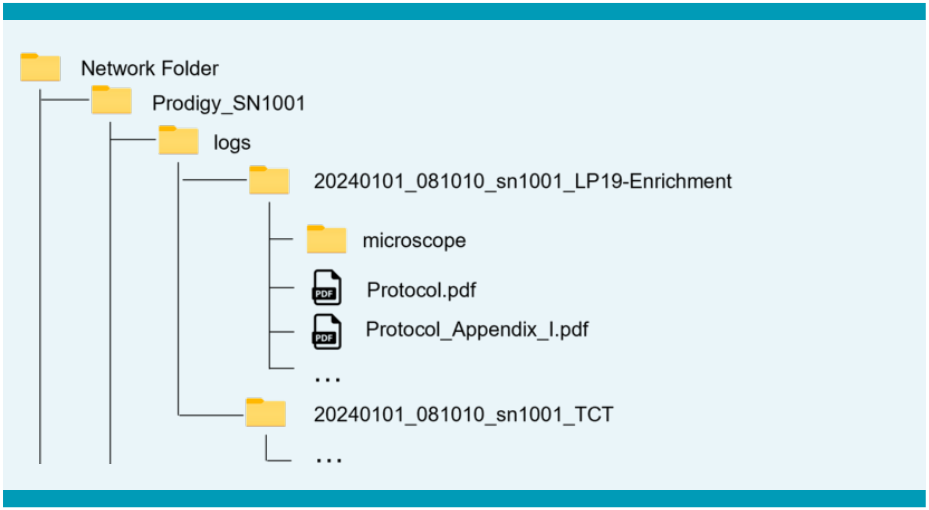


Abbildung 7.2: Dateistruktur im File Sharing

WICHTIG

Die Protokolldateien im Gerät sind durch Zugriffskontrolle geschützt, um sicherzustellen, dass nur berechtigte Personen darauf zugreifen können. Wenn diese Dateien in ein Netzlaufwerk übertragen werden, liegt es in der Verantwortung des Anwenders, geeignete Maßnahmen zur Zugriffsbeschränkung zu treffen.

7.2 Abrufen des Audit-Trails

Das Audit-Trail-System zeichnet sämtliche Benutzerinteraktionen mit der Software auf. Jede Benutzerinteraktion führt zu einer Audit-Trail-Aufzeichnung mit Benutzer-ID, Zeitstempel und Beschreibung der Interaktion. Der Audit-Trail kann im .pdf- oder .csv-Format exportiert werden. Tabelle 7.1 zeigt das Audit-Trail-Format.

WICHTIG

Der Zeitstempel der Audit-Trail-Aufzeichnung ist immer die UTC-Zeit.

Time (Zeit)	Kategorie	Typ	User	Description
2020-Jul-21 10:33:44	User interaction	Pop-up close	AccountID	Progress paused 'warning'
...	...	...	...	...

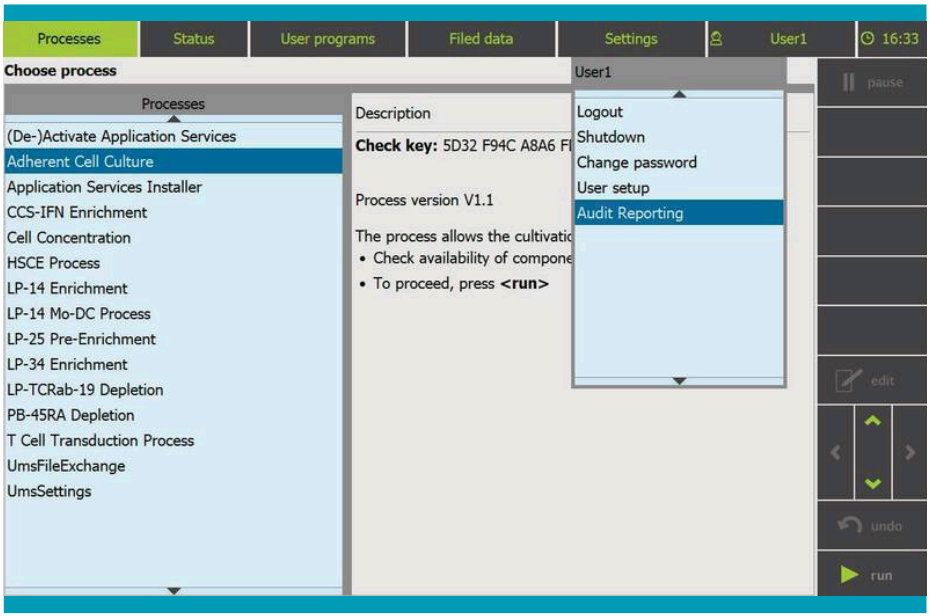
Tabelle 7.1: Audit-Trail-Format

Anmerkung: Die Rolle 'ATS User' oder eine Rolle mit Rechten des 'Audit Trail Management' ist erforderlich, um das Audit-Trail-System aufzurufen.

- Die Rolle 'ATS User' hat vollständigen Zugriff mit den Rechten, Audit-Trail-Aufzeichnungen anzuzeigen, zu exportieren und zu löschen.
- Eine neue Rolle mit begrenztem Zugriff auf Audit-Trail-Funktionen kann angelegt werden. Nähere Einzelheiten zur Konfiguration von Rollen und Rechten finden Sie in Kapitel 10 ´Benutzerverwaltung´.

7.2.1 Anzeigen des Audit-Trails

Um den Audit-Trail zu öffnen, gehen Sie zu ▸ **<Audit Reporting>** (siehe Bildschirm 7.3). Das Menü **<Audit Trail>** enthält eine Liste aller verfügbaren Audit-Trail-Ereignisse auf dem Gerät (siehe Abbildung 7.3).



Bildschirm 7.3: Audit Reporting

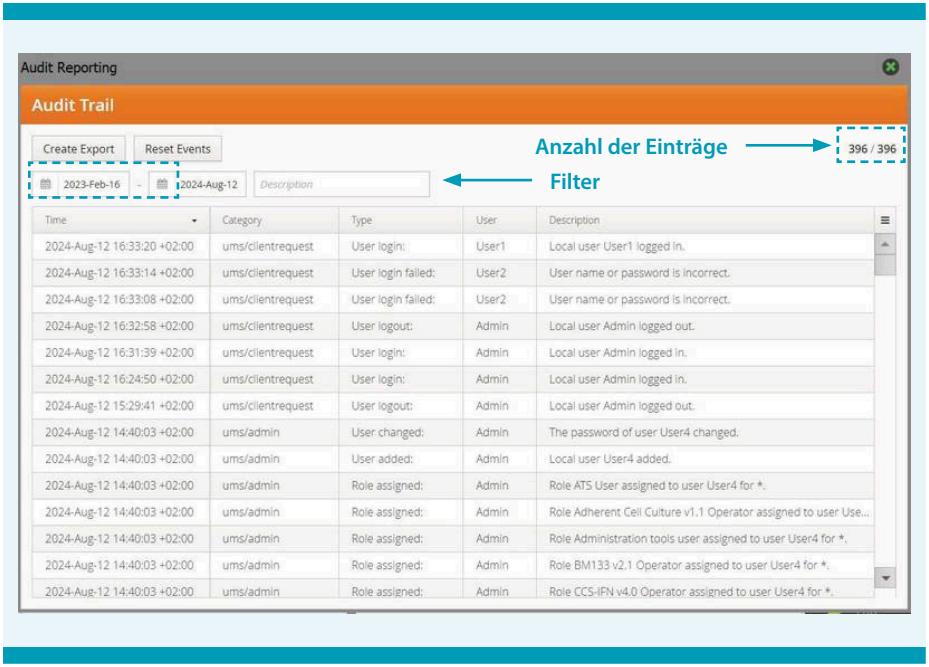
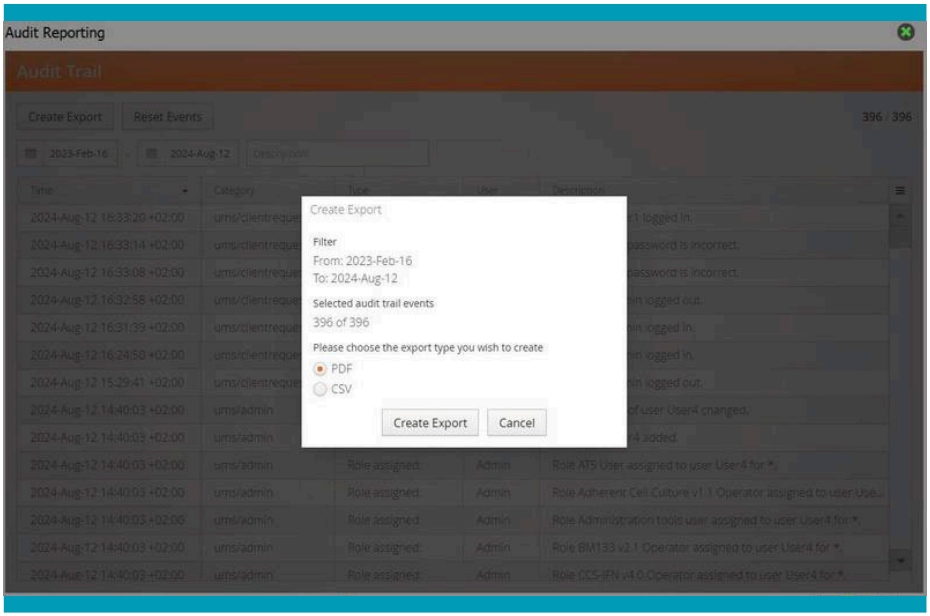


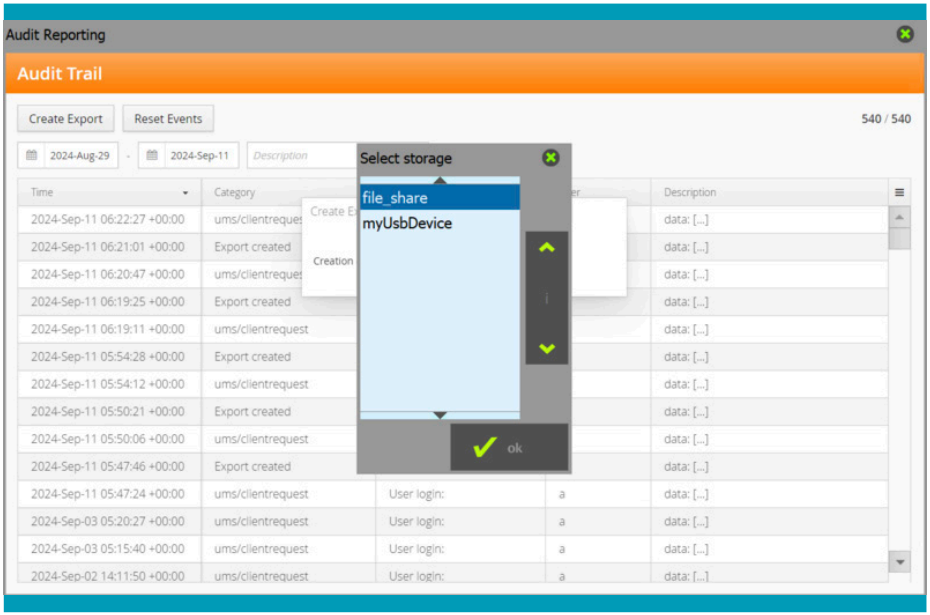
Abbildung 7.3: Menü Audit Trail

7.2.2 Exportieren des Audit-Trails

1. Die Filterkriterien eingeben in die Felder in Abbildung 7.3. Wenn keine Kriterien eingegeben wurden, werden alle Audit-Trail-Aufzeichnungen exportiert.
2. Auf **<Create Export>** über den Filterkriterien drücken. Ein Pop-up-Fenster wird angezeigt (Bildschirm 7.4).
3. Im Pop-up-Fenster das Format wählen und **<Create Export>** drücken.
4. Wenn mehrere Speicherorte festgestellt werden, z. B. wenn File Sharing konfiguriert ist und ein USB-Stick eingesteckt wird, muss der Speicherort gewählt werden (Bildschirm 7.5).



Bildschirm 7.4: Erstellen des Audit-Trail-Exports



Bildschirm 7.5: Wählen des Speicherortes für den exportierten Audit-Trail

5. Warten, bis der Vorgang beendet ist, und überprüfen, ob die Datei exportiert wurde.

7.2.3 Löschen des Audit-Trails

1. Um alle Audit-Trail-Einträge zu löschen, auf **<Reset Events>** (Ereignisse zurücksetzen) drücken.

2. Mit **<Continue Reset>** bestätigen. Nach dem Zurücksetzen werden alle Aufzeichnungen gelöscht. Eine neue Aufzeichnung für den Löschvorgang wird gespeichert.

WICHTIG

Es ist nicht möglich, einzelne Einträge zu löschen. Gelöschte Daten können nicht wiederhergestellt werden. Achten Sie darauf, dass nur berechtigte Benutzer das Recht zum Löschen des Audit-Trails haben. Informationen zum Konfigurieren von Rollen und Rechten finden Sie im Kapitel 10 ´Benutzerverwaltung´.

8

Tools und Benutzereinstellungen

8.1 Zugriff auf Tools und Benutzereinstellungen

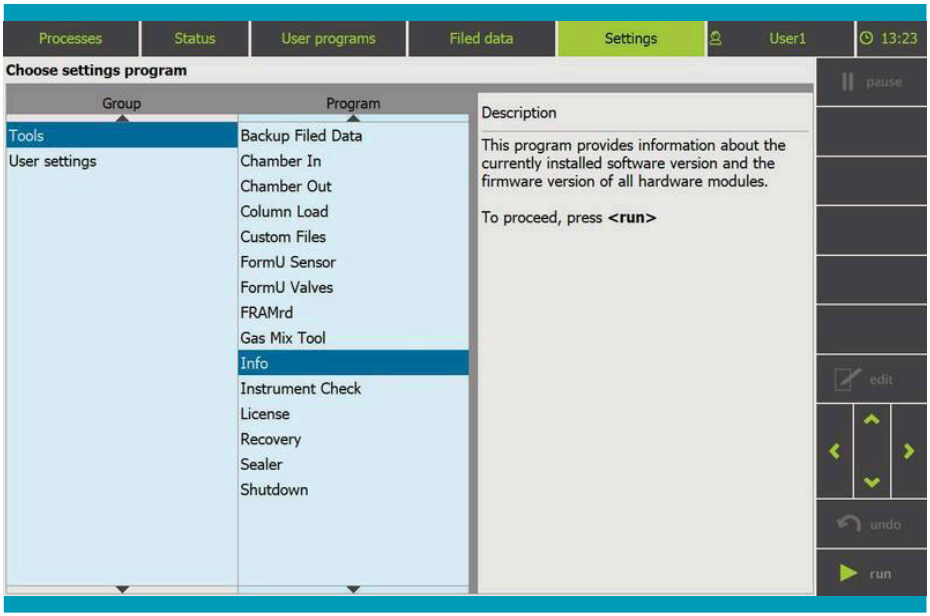
Im Menü **<Settings>** gibt es zwei Arten von Programmen: Tools und Einstellungen.

Anmerkung: Tools und Einstellungen sind während eines laufenden Prozesses nicht verfügbar.

So finden und aktivieren Sie ein Tool bzw. eine Einstellung:

1. Die Option **<Tools>** oder **<User settings>** aus der Liste **<Gruppe>** wählen. Siehe Bildschirm 8.1.
2. Auf das gewünschte Programm in der Liste **<Programm>** drücken. Das gewählte Programm wird blau hinterlegt. Im Feld **<Beschreibung>** finden Sie ausführliche Informationen über das gewählte Tool bzw. die gewählte Einstellung. Durch Drücken auf ^ und v in der Prozessliste können weitere verfügbare Optionen angezeigt werden. Alternativ kann das gewünschte Programm mit den Navigationstasten ausgewählt werden.
3. Um das ausgewählte Programm zu starten, auf **<run>** in der Werkzeugleiste drücken.

In den folgenden Abschnitten werden häufig verwendete Tools und Benutzereinstellungen vorgestellt.



Bildschirm 8.1: Auswählen eines Tools oder einer Einstellung

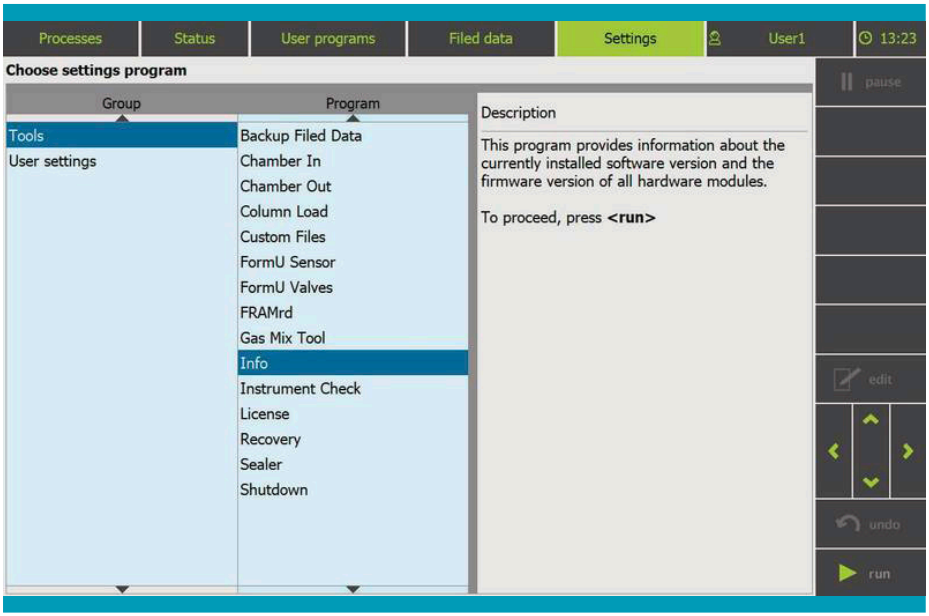
8.2 Tools

Alle Tools finden Sie unter **<Settings>** ▸ **<Tools>**.

8.2.1 Info tool

Das Tool Info liefert ausführliche Informationen über die Software und Hardware. Die wichtigsten Informationen sind:

- Softwareversion
- Build-Nummer
- Firmwareversion
- Nutzung der Festplatten-Speicherkapazität mit Angabe von freiem Speicherplatz, belegtem Speicherplatz und Gesamtkapazität
- IP-Adresse
- MAC-Adresse
- Vollständige Laufzeitinformationen (für alle Anwendungen und Tools) sowie der Leerlaufzeit (Zeit, in der keine Anwendung auf dem Gerät lief)



Bildschirm 8.2: Das Tool Info

8.2.2 Backup Filed Data (Datensicherung für Dateien)

Das Tool 'Backup Filed Data' kopiert alle Prozessdaten an einen Sicherungsspeicherort oder löscht alle Prozessdaten.

WICHTIG

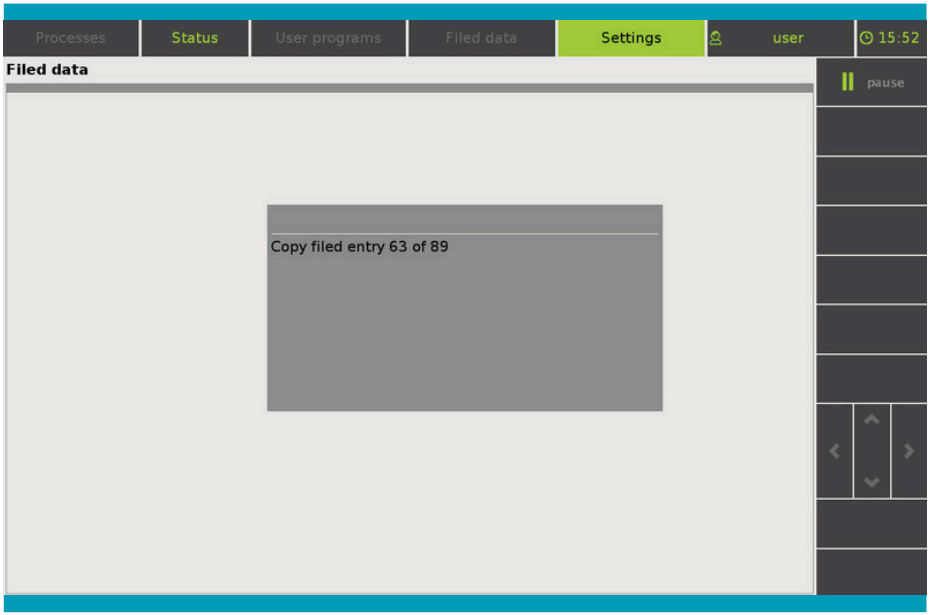
- Es wird empfohlen, die Prozessdaten regelmäßig zu sichern. Andernfalls kann eine Benutzeraufforderung erscheinen, die darauf hinweist, dass das Programm nicht gestartet werden darf, da die maximale Speicherkapazität für archivierte Daten erreicht wurde.
- Bei Verwendung eines USB-Sticks für das Backup muss der USB-Stick im Format FAT 32 sein und darf nicht passwortgeschützt sein.
- Wenn File Sharing konfiguriert ist, können Dateien auch in den File-Sharing-Ordner exportiert werden (siehe Abschnitt 9.3 ´Verbindung zu einem Netzlaufwerk herstellen´).

Kopieren von Daten

1. Einen USB-Stick einstecken.
2. Zu <Settings > ▸ <Tools> ▸ <Backup Filed Data> gehen und auf <run> drücken.
3. Bei der Eingabeaufforderung <Backup> wählen (siehe Bildschirm 8.3). Das Kopieren der Daten startet (siehe Bildschirm 8.4).



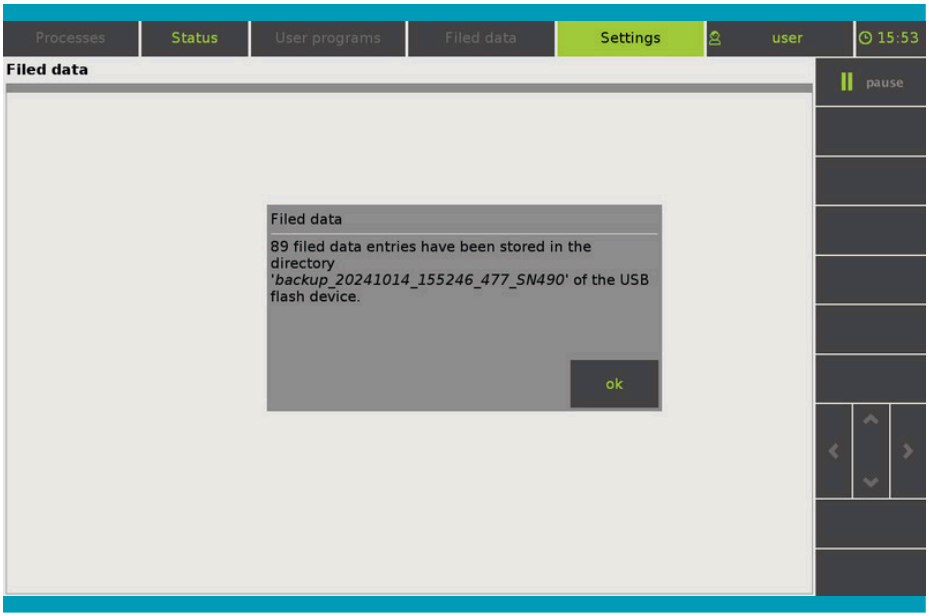
Bildschirm 8.3: Backup wählen



Bildschirm 8.4: Datensicherungsvorgang

4. Warten, bis die Dateien kopiert sind. Dann bei der Meldung über den Abschluss der Sicherung auf <ok> drücken (siehe Bildschirm 8.5).

5. Überprüfen, ob die Dateien vollständig gesichert wurden.



Bildschirm 8.5: Datensicherung abgeschlossen

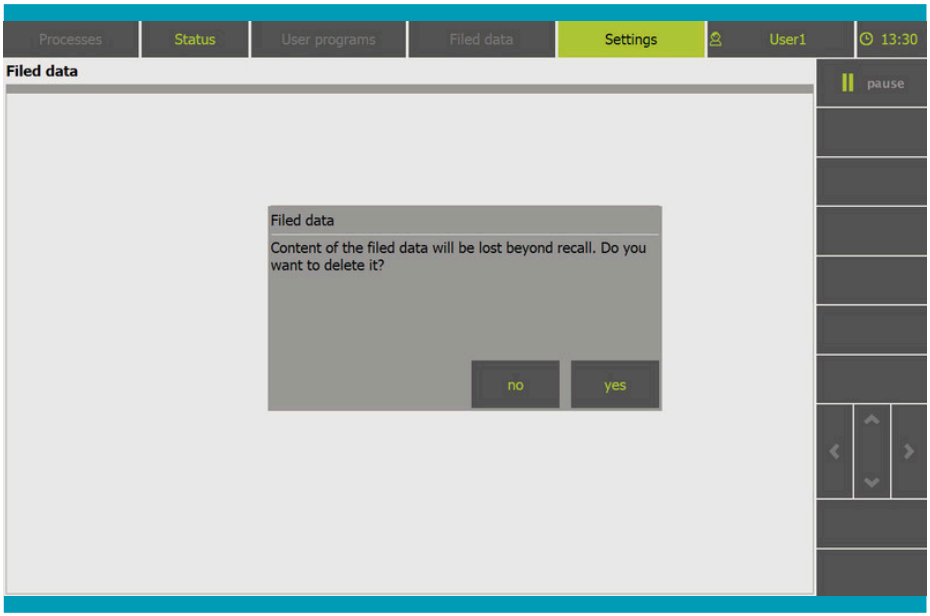
Löschen von Daten

1. Überprüfen, ob die Dateien vollständig gesichert wurden.
2. Zu <Settings> ▸ <Tools> ▸ <Backup Filed Data>, gehen und auf <run> drücken.
3. Auf <Delete> drücken (siehe Bildschirm 8.6).



Bildschirm 8.6: Löschen wählen

4. Zur Bestätigung auf <yes> drücken (siehe Bildschirm 8.7).

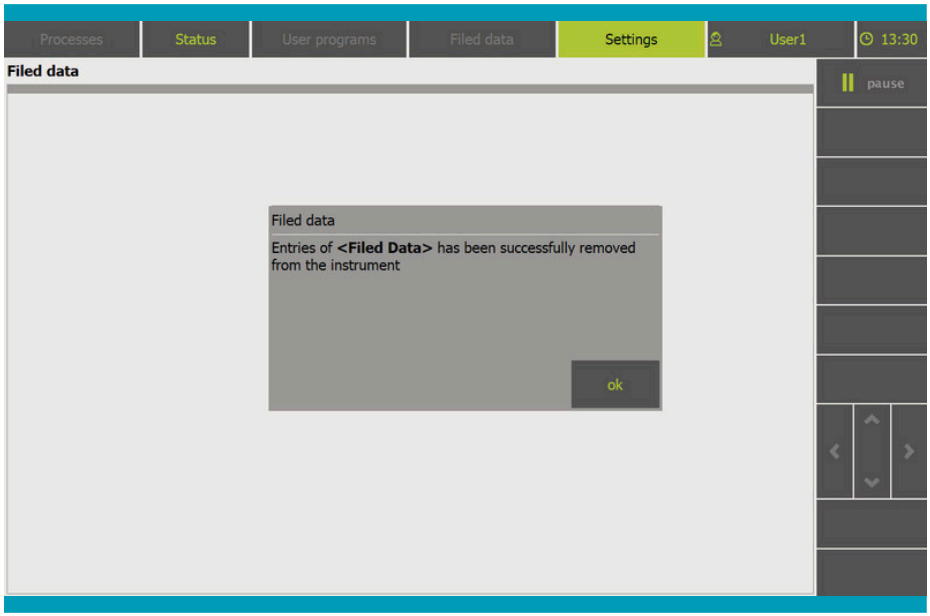


Bildschirm 8.7: Löschen von Daten bestätigen

5. Warten, bis der Löschvorgang abgeschlossen ist. Dann bei der entsprechenden Meldung auf **<ok>** drücken (siehe Bildschirm 8.8).

6. Nach dem Löschvorgang sind alle Aufzeichnungen unter **<Filed Data>** gelöscht. Eine Aufzeichnung über die Ausführung des Tools **<Backup Filed Data>** wird erstellt.

WICHTIG
Gelöschte Daten können nicht wiederhergestellt werden.



Bildschirm 8.8: Löschvorgang abgeschlossen

8.2.3 Chamber In (Kammer rein)

Dieses Tool wird verwendet, um die CentriCult-Einheit außerhalb einer laufenden Anwendung einzusetzen. Der Kammerverriegelungsadapter schaltet in die Einsetzposition und entriegelt die Haube der CentriCult-Einheit. Öffnen Sie nach Verwendung dieses Tools die CentriCult-Einheit manuell.

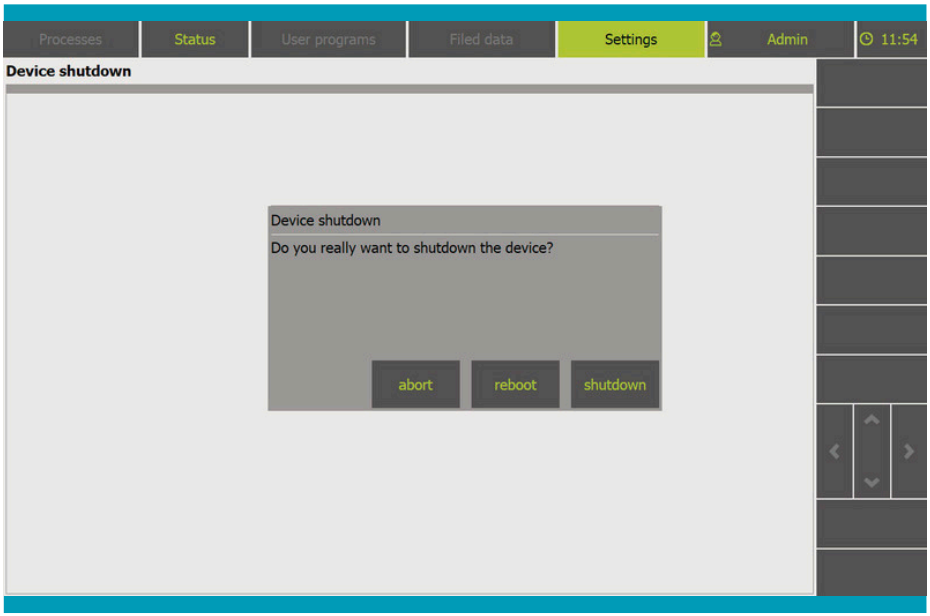
8.2.4 Chamber Out (Kammer raus)

Dieses Tool wird verwendet, um die CentriCult-Einheit außerhalb einer laufenden Anwendung auszutauschen. Der Kammerverriegelungsadapter schaltet in die Austauschposition und entriegelt die Haube der CentriCult-Einheit. Öffnen Sie nach Verwendung dieses Tools die CentriCult-Einheit manuell.

8.2.5 Shutdown

Dieses Tool schaltet das Gerät aus oder startet es neu.

1. Auf <run> in der Werkzeugleiste drücken, um die Aussschaltfunktion auszuführen.
2. Abort (Abbrechen), Shutdown (Ausschalten) oder Reboot (Neu starten) wählen (siehe Bildschirm 8.9).



Bildschirm 8.9: Shutdown (Ausschalten) oder Reboot (Neu starten) wählen

8.2.6 Recovery (Rückgewinnung)

Dieses Programm ermöglicht die Rettung von Zellprodukten in speziellen Beuteln nach einer Prozessstörung. Dieses Tool unterstützt nur die folgenden CliniMACS Prodigy Schlauchsets: TS 310, TS 500 und TS 510.

WICHTIG

Verwenden Sie dieses Tool nur unter Anleitung des Miltenyi Biotec Technical Supports.

8.2.7 Gas Mix tool (Gasmisch-Tool)

Dieses Programm ermöglicht die Gasprobenahme mit einem Probenbeutel aus der Gasmischeinheit.

8.2.8 Instrument Check tool (Geräteprüfung)

Dieses Tool führt eine halbautomatisierte Geräteprüfung durch, bei der eine Benutzerinteraktion erforderlich ist.

8.2.9 Column Load (Säulenbeladung)

In einigen bestimmten Fällen ermöglicht der Prozess die Anreicherung von CD34-positiven Zellen aus Leukapheresat.

8.2.10 Custom Files (benutzerdefinierte Dateien)

Dieses Programm wird verwendet, um CAPs in das Gerät aufzunehmen.

8.2.11 Sealer (Schlauchschweißgerät)

Dieses Programm dient dazu, das Schlauchschweißgerät (Sealer) ein- und auszuschalten.

8.3 User settings (Benutzereinstellungen)

Diese Einstellungen finden Sie unter **<Settings>** ▸ **<User settings>**.

8.3.1 Set time (Uhrzeit einstellen)

Diese Funktion dient dazu, das Datum und die Uhrzeit des Geräts einzustellen.

Anmerkung: Die hier eingestellte Zeit wird automatisch überschrieben, wenn die Netzwerk-Zeitsynchronisation aktiviert ist. Informationen zur Einstellung der Netzwerk-Zeitsynchronisation finden Sie im Abschnitt 9.6 ´Aktivieren der Netzwerk-Zeitsynchronisation´.

8.3.2 Network settings (Netzwerkeinstellungen)

Diese Einstellung enthält die notwendigen Informationen für die Netzwerkintegration. Ausführliche Erläuterungen sind in den folgenden Abschnitten zu finden:

- 9.1 zur Netzwerkintegration
- 9.2 zur LDAP-Verbindung
- 9.3 zum File Sharing
- 9.4 zur Dateiübertragung über FTP
- 9.6 zur Netzwerk-Zeitsynchronisation

Informationen zur Einrichtung von E-Mail-Benachrichtigungen finden Sie in Abschnitt 9.5 ´Verbinden mit einem E-Mail-Server´

8.3.3 Custom settings (Benutzerdefinierte Einstellungen)

Benutzerdefinierte Einstellungen sind allgemeine Einstellungen für das Gerät, wie zum Beispiel Sprache, Firmenname, Abteilung, Straße, Postleitzahl, Ort, Gerätename, Kontaktperson, Standort.

Die Einstellung der E-Mail-Benachrichtigung finden Sie ebenfalls unter den benutzerdefinierten Einstellungen, siehe Abschnitt 9.5 ´Verbinden mit einem E-Mail-Server´.

8.3.4 Module Settings (Einstellungen für die Module)

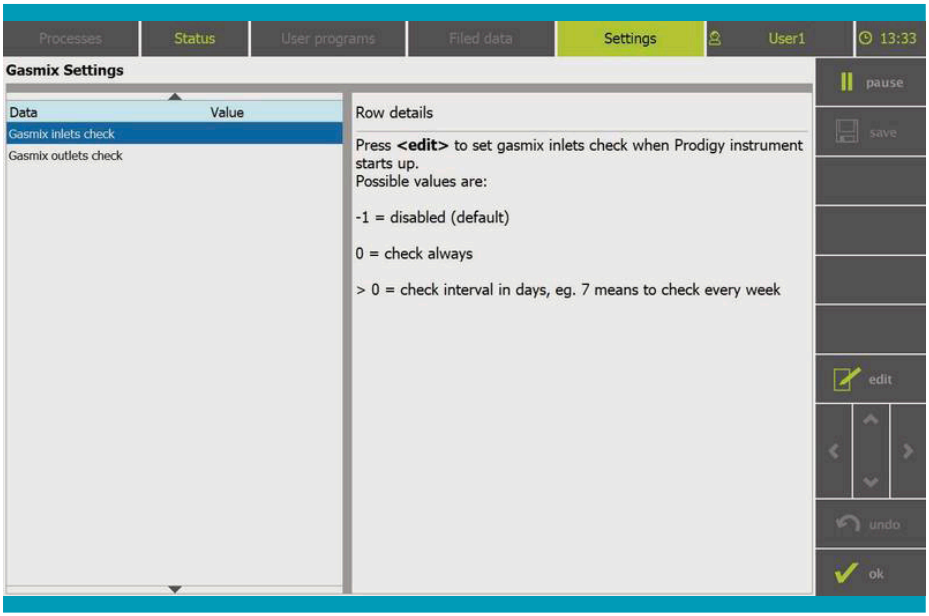
Die Module Settings enthalten Konfigurationen für Hardwaretests, darunter:

- Kontrolle der Gasmix-Eingänge
- Kontrolle der Gasmix-Ausgänge
- Kontrolle der Rotation
- Erinnerung an den Supplementary Bag

Für jede dieser Komponenten kann die Durchführung von Kontrollen in verschiedenen zeitlichen Abständen eingestellt werden:

- Nie (-1)
- Immer (0)
- Regelmäßig (Abstand in Tagen eingeben).

Eine Beispielkonfiguration der Gasmix-Eingänge siehe Bildschirm 8.10.



Bildschirm 8.10: Kontrolle der Gasmix-Eingänge

8.3.5 Tool Settings Exchange (Austausch von Einstellungen)

Das Tool <Settings Exchange> ermöglicht es, Konfigurationen in mehrere Geräte zu kopieren. Dies gilt für folgende Einstellungen:

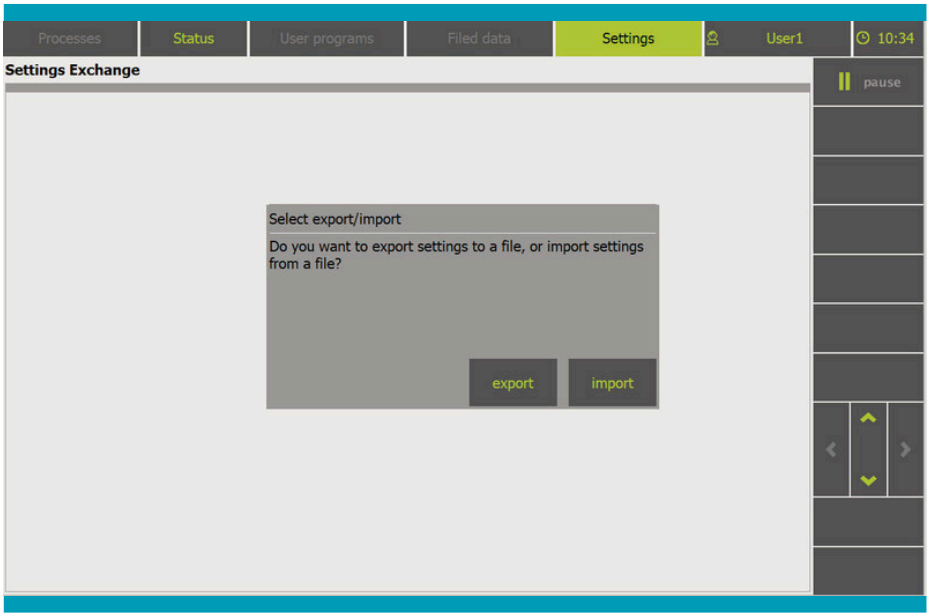
- Customer settings (benutzerdefinierte Einstellungen)
- Gasmix settings (Einstellungen für die Gasmischung)
- Module settings (Einstellungen für die Module)
- Network settings (Netzwerkeinstellungen)

WICHTIG

- Bei Verwendung eines USB-Sticks zum Importieren oder Exportieren muss der USB-Stick im Format FAT 32 sein und darf nicht passwortgeschützt sein.
- Wenn File Sharing konfiguriert ist (siehe Abschnitt 9.3 ´Verbindung zu einem Netzlaufwerk herstellen´), können Dateien auch in den File-Sharing-Ordner exportiert werden.

Exportieren der Einstellungen auf USB-Stick

1. Einen USB-Stick einstecken.
2. Zu <Settings> ▸ <User settings> ▸ <Setting Exchange> gehen und auf <run> drücken.
3. In der angezeigten Aufforderung auf <export> drücken (siehe Bildschirm 8.11).



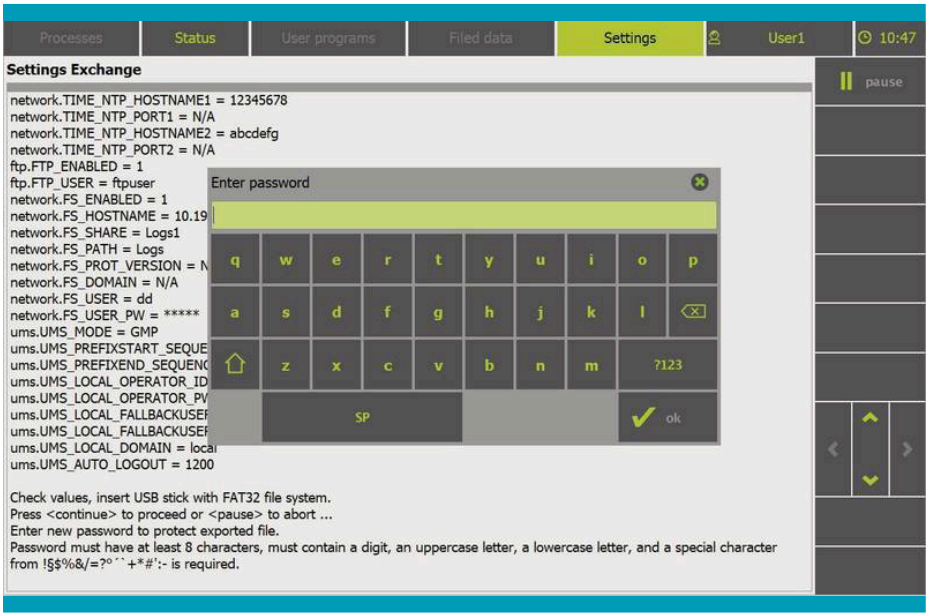
Bildschirm 8.11: Export wählen

4. Die Werte auf dem Bildschirm überprüfen. Auf <continue> in der Werkzeugleiste drücken.



Bildschirm 8.12: Einstellungswerte überprüfen

5. Das Login-Passwort eingeben.



Bildschirm 8.13: Passwort eingeben

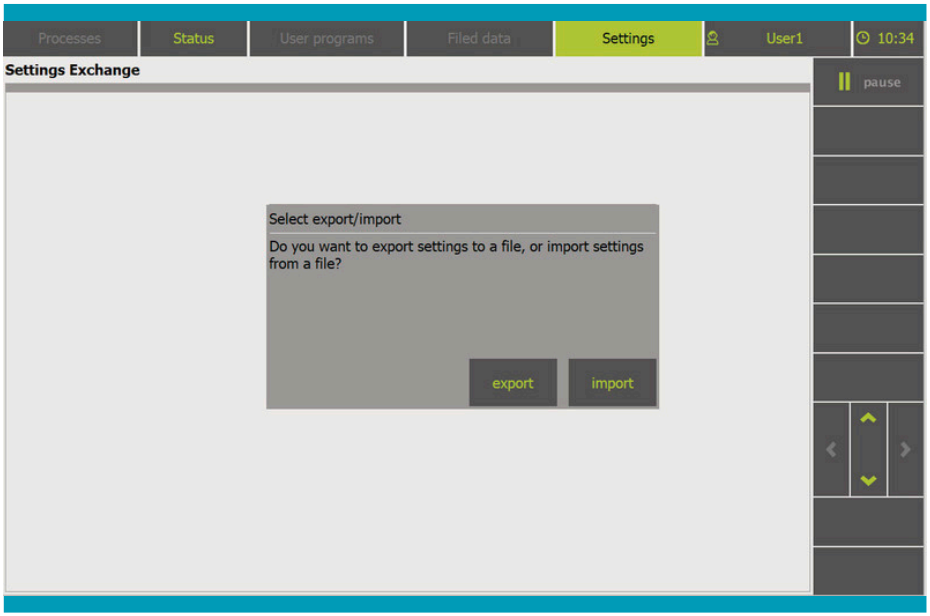
Importieren der Einstellungen von einem USB-Stick

1. Einen USB-Stick mit der gewünschten Datei mit Benutzereinstellungen einstecken.

   Anmerkung: Der USB-Stick muss im Format FAT 32 formatiert sein und darf nicht passwortgeschützt sein.

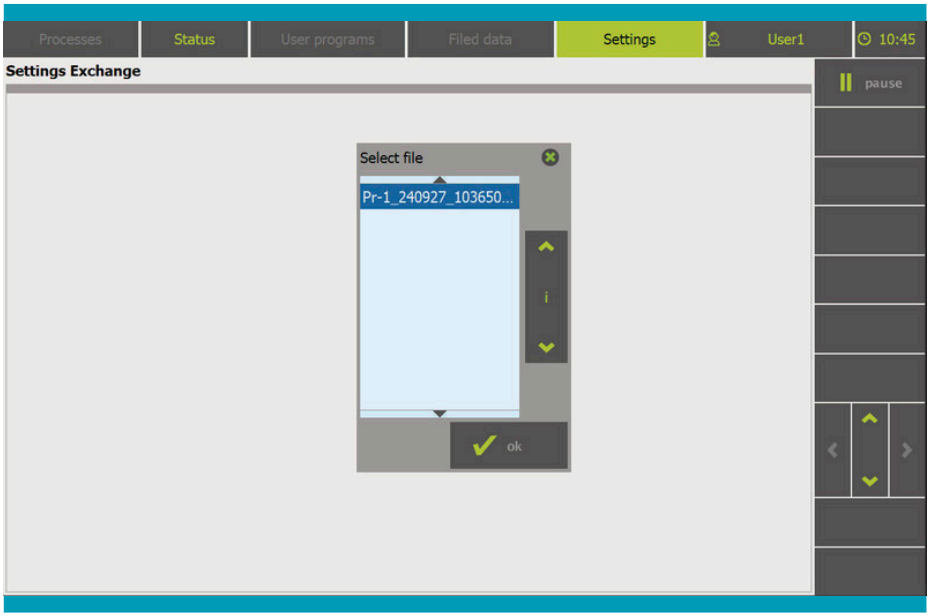
2. Zu **<Settings>** ▸ **<User settings >** ▸ **<Setting Exchange>** gehen und auf **<run>** drücken.

3. In der angezeigten Aufforderung auf **<Import>** drücken (siehe Bildschirm 8.14).



Bildschirm 8.14: Import wählen

4. Die zu importierenden Dateien wählen und auf <ok> drücken (siehe Bildschirm 8.15).



Bildschirm 8.15: Wählen der zu importierenden Datei

5. Das Login-Passwort eingeben (siehe Bildschirm 8.13).

8.3.6 SetVolume (Volumen einstellen)

Dieses Programm stellt die Lautstärke des Lautsprechers des Geräts ein.

8.3.7 N_2 Settings (N_2-Einstellungen)

Dieses Programm konfiguriert, welche beiden der drei Gasanschlüsse des Geräts verwendet werden (N_2, CO_2 Druckluft).

9 Netzwerkintegration

Das Gerät kann mithilfe eines USB-Ethernet-Adapters mit dem lokalen Netzwerk verbunden werden. Eine geeignete Netzwerkintegration ist zur Verwendung der folgenden Funktionen erforderlich:

- Zentralisierte Benutzerverwaltung (LDAP)
- Dateiübertragung über FTP
- Automatisches File Sharing
- E-Mail-Benachrichtigung
- Netzwerk-Zeitsynchronisation

Zur Verwendung der oben genannten Funktionen verbinden Sie das Gerät zuerst mit dem lokalen Netzwerk. Informationen dazu finden Sie in Abschnitt 9.1 ´Verbinden mit einem lokalen Netzwerk´. Folgen Sie dann den Anweisungen für die jeweiligen Funktionen.

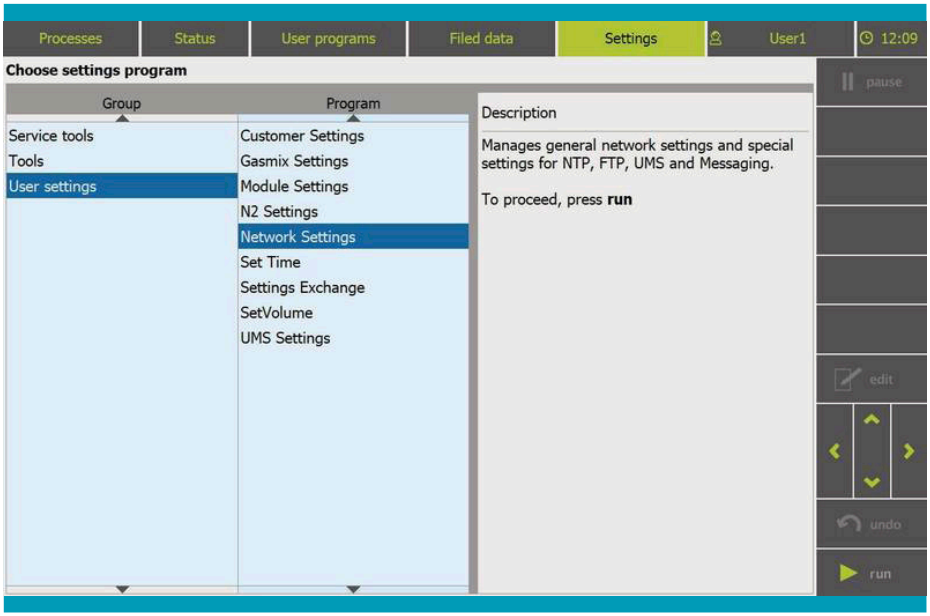
WICHTIG

- Nur UMS-Benutzer mit der Administratorrolle 'Administration tools user' oder Benutzer mit 'Network Setting'-Rechten haben Zugang zu dieser Einstellung. Informationen zum Konfigurieren von Rechten und Rollen finden Sie im Kapitel 10 ´Benutzerverwaltung´.
- Die Schaltfläche **<Connectivity Hub>** kann auf dem Bildschirm angezeigt werden. Diese ist jedoch zurzeit noch inaktiv, bis die Funktion unterstützt wird.

- Der Anwender muss sicherstellen, dass die Firewall-Einstellungen den Datenaustausch zwischen dem Gerät und dem gewünschten Server/Client erlauben. Der Kunde ist für die Konfiguration der Firewall-Einstellungen verantwortlich.
- Bei manchen Einstellungen muss das Gerät neu gestartet werden, damit die Änderungen wirksam werden.

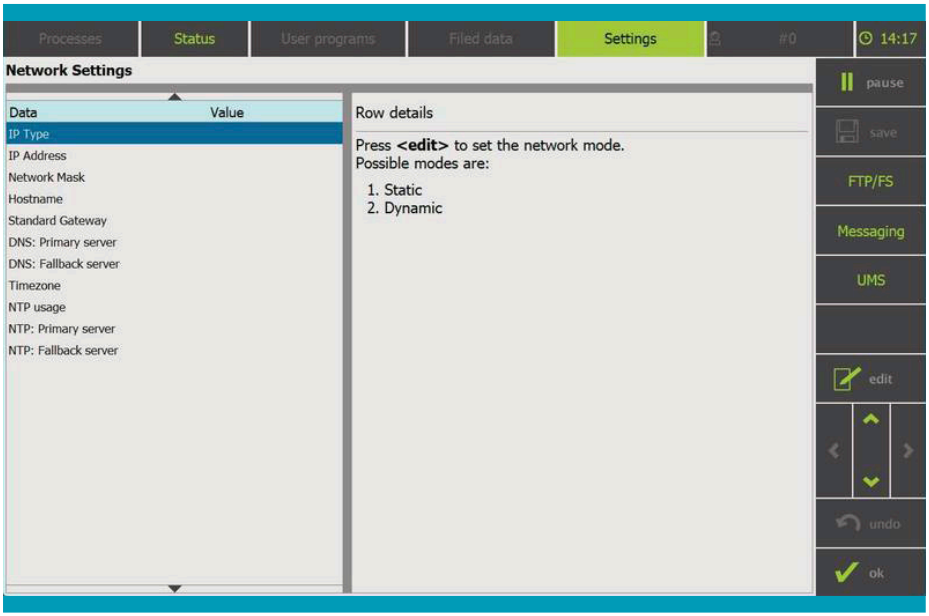
9.1 Verbinden mit einem lokalen Netzwerk

1. Das Gerät mithilfe eines USB-Ethernet-Adapters mit dem lokalen Netzwerk verbinden.
2. Um die Netzwerkeinstellungen einzugeben, zu **<Settings>** ▸ **<User settings>** ▸ **<Network Settings>** gehen und auf **<run>** drücken (siehe Bildschirm 9.1). Die Netzwerkeinstellungen werden angezeigt (Bildschirm 9.2).



Bildschirm 9.1: Wählen der Netzwerkeinstellungen

3. Um zwischen statischer IP-Adresse und dynamischer IP-Adresse zu wählen, **<IP Type>** aus der Liste wählen und auf **<edit>** in der Werkzeugleiste drücken. Dann den gewünschten Wert in das Eingabefeld eingeben.



Bildschirm 9.2: Network settings (Netzwerkeinstellungen)

Für eine statische IP-Adresse die folgenden Schritte durchführen:

1. < IP-Adress > in der Liste auswählen, in der Werkzeugleiste auf <edit> drücken und die IP-Adresse in das Eingabefeld eingeben.
2. <Network Mask> aus der Liste auswählen, auf <edit> drücken und die Netzwerkmaske in das Eingabefeld eingeben.
3. Um den Namen des Geräts einzugeben, <Hostname> wählen und auf <edit> drücken.
4. Zur Eingabe der IP-Adresse des Gateways <Standard Gateway> wählen und auf <edit> drücken.
5. Optional: Um die Zeitzone auszuwählen, <Timezone> wählen und auf <edit> drücken. Die Standardzeitzone des Geräts ist die koordinierte Weltzeit (Universal Time Coordinated, UTC).
6. Überprüfen, ob das Gerät mit dem lokalen Netzwerk verbunden ist.

Für eine dynamische IP-Adresse die folgenden Schritte durchführen:

1. Um den Namen des Geräts einzugeben, <Hostname> wählen und auf <edit> drücken.
2. Der dynamische Server muss konfiguriert werden. Eine IP-Adresse für den Haupt- (primary) und den Ersatz-Server (fallback) eingeben.
3. Optional: Um die Zeitzone auszuwählen, <Timezone> wählen und auf <edit>

drücken. Die Standardzeitzone des Geräts ist die koordinierte Weltzeit (Universal Time Coordinated, UTC).

4. Überprüfen, ob das Gerät mit dem lokalen Netzwerk verbunden ist.

WICHTIG

Wenn die Netzwerk-Ports in Ihrem Unternehmen durch MAC-Adressfilter gesichert sind, fragen Sie Ihren örtlichen IT-Dienstleister nach der korrekten Einrichtung.

9.2 Verbindung zu einem LDAP-Server herstellen

Um die Verbindung zum LDAP-Server zu konfigurieren, zum (Schnellzugriffsmenü) gehen und <User Management> wählen. Im Menü <User Management> die Option <Configuration> ▸ <LDAP Configuration> wählen. Zur Konfiguration von LDAP die folgenden Schritte durchführen (siehe Abbildung 9.1).

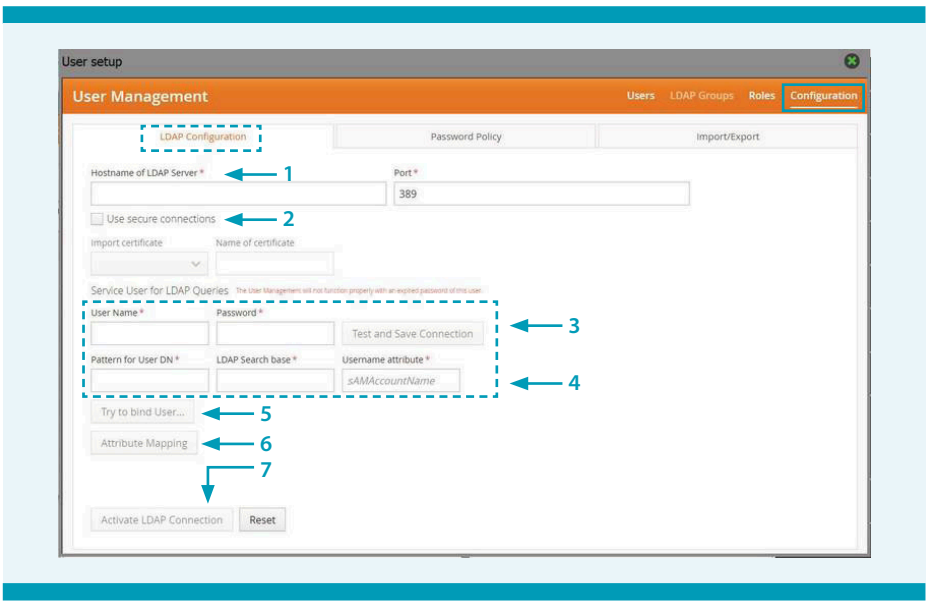


Abbildung 9.1: Menü User Management und Schritte zur Konfiguration von LDAP

1. Den Hostnamen/IP-Adresse des LDAP-Servers eingeben.
2. Eine sichere Verbindung wählen, falls erforderlich. Dadurch wird automatisch der Standardport 389 auf den Port 636 für eine sichere LDAP-Verbindung eingestellt. Für eine sichere Verbindung den Anweisungen in Abschnitt 10.4.2 folgen, um das Certificate in das Prodigy-Gerät zu importieren. Hierzu das Certificate in der Dropdown-Liste unter <import certificate> wählen.
3. Den Benutzernamen und das Passwort eines gültigen LDAP-Kontos eingeben.

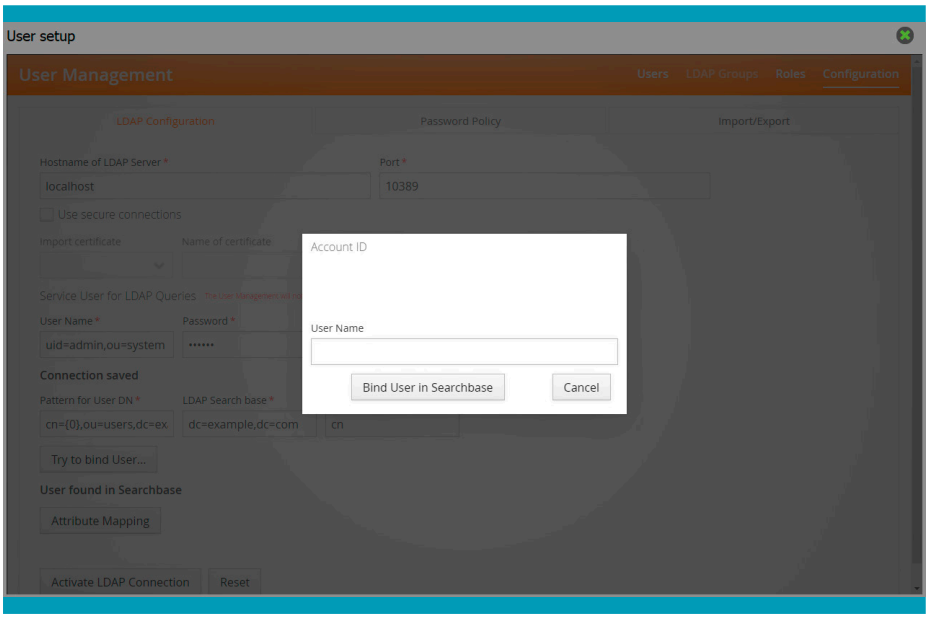
Der vollständige LDAP-Pfad des Benutzernamens sollte eingegeben werden. Auf <Test and Save Connection> (Verbindung testen und speichern) drücken. Ein Pop-up-Fenster erscheint mit der Meldung, dass die Verbindung erfolgreich hergestellt wurde.

4. Das Pattern, die Search Base und das Benutzernamen-Attribut eingeben. Das Pattern für den Benutzer-Domainnamen sollte den vollständigen Pfad enthalten. Diese Einträge sind abhängig von der LDAP-Organisationsstruktur und dem Domainnamen des Benutzers. Eine kurze Erläuterung und Beispiele von typischen Werten werden angezeigt, wenn Sie über die Textfelder fahren. Es kann hilfreich sein, wenn jemand mit Zugang zu einem LDAP-Browserprogramm die Organisationseinheiten darin zeigt.

   Typische Werte sind so etwas wie:

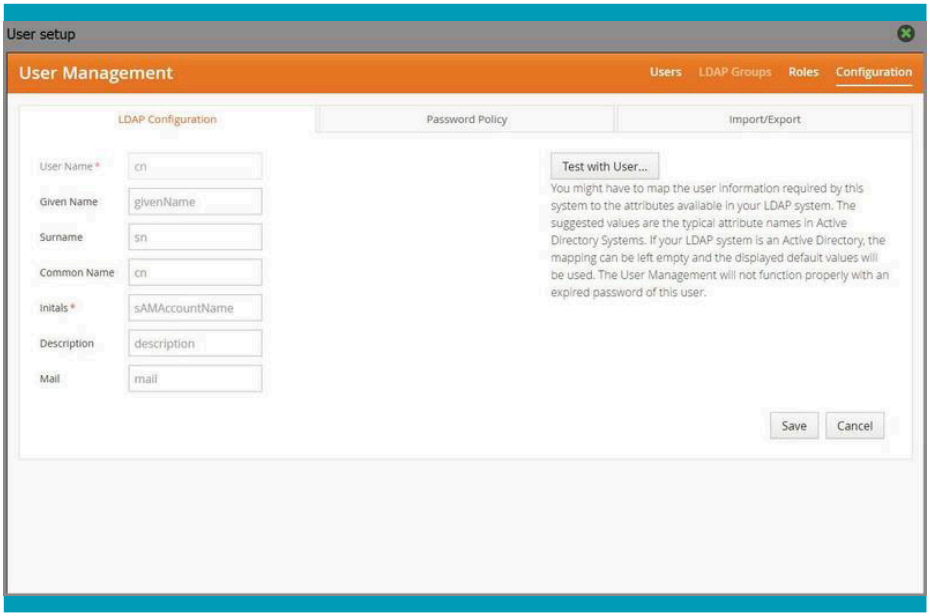
   - Pattern = '<domain>/{0}', zum Beispiel 'Kundenname_dev/{0}'
   - Search base = 'OU=Organisation,DC=Kundenname'
   - Benutzername-Attribut = 'sAMAccountName'

5. Auf <Try to bind User....>. Ein Pop-up-Fenster wird angezeigt (Bildschirm 9.3). Einen gültigen Benutzernamen eingeben (kann derselbe wie der beim Login-Test verwendete sein). Dann auf <Bind User in Searchbase> drücken, um fortzufahren. Falls erfolgreich, wird das Pop-up-Fenster Account ID geschlossen. Anderenfalls wird eine Fehlermeldung angezeigt.



Bildschirm 9.3: Pop-up-Eingabefenster Account ID zur Eingabe eines gültigen Benutzernamens

6. Auf <Attribute Mapping> drücken. Das Attribut-Mapping wird angezeigt (Bildschirm 9.4). Das in Schritt 4 eingegebene Benutzernamen-Attribut wird automatisch dem Benutzernamen zugeordnet. Denselben Wert für die Initialen wie für den Benutzernamen eingeben. Die hier eingegebenen Werte erscheinen automatisch in einigen Feldern, wenn ein Benutzer angelegt wird. Auf <save> drücken, um zur LDAP-Konfigurationsseite zurückzukehren.
7. Auf <Activate LDAP Connection> drücken. Diese Schaltfläche ist aktiv, wenn die Schritte 3, 4 und 5 erfolgreich waren.



Bildschirm 9.4: Beispiel für vorab ausgefüllte Attribute

WICHTIG

Es ist notwendig, einen Wert für 'Initials' (siehe Bildschirm 9.4) einzustellen, da dieser Wert als Pflichtangabe für Benutzer des CliniMACS Prodigy gilt. Eine fehlende oder falsche Konfiguration der Attributübersicht kann zum Fehlschlag des Logins führen.

Mit den vorstehenden sieben Schritten (siehe Abbildung 9.1) kann die LDAP-Verbindung vollständig konfiguriert und jetzt zum Anlegen von LDAP-Gruppen und LDAP-Benutzern unter <User Management> verwendet werden. Weitere Einzelheiten zum Verwalten von Benutzerkonten und Rollen finden Sie im Kapitel 10 ´Benutzerverwaltung´.

9.3 Verbindung zu einem Netzlaufwerk herstellen

Das automatische File Sharing schiebt alle Protokolldateien unmittelbar nach Abschluss des Prozesslaufs der Applikation auf das Netzlaufwerk. Die Audit-Trail-Aufzeichnungen können vom Anwender manuell ebenfalls auf das Netzlaufwerk exportiert werden (siehe Abschnitt 7.2.2 ´Exportieren des Audit-Trails´). Die automatische Dateiübertragung ist auf der Basis des Protokolls Server Message Block (SMB) implementiert. Die Versionen SMB 1.0, SMB 2.1 und SMB 3.0 (Standard) des SMB-Protokolls werden unterstützt.

Anmerkung: SMB 2.0 und SMB 3.0 werden empfohlen. SMB 1.0 wird nur zur Verwendung für Altsysteme unterstützt und sollte nur zur Interaktion mit Altsystemen verwendet werden.

Voraussetzungen

- SMB-Server: Achten Sie darauf, dass dieser SMB-Server erreichbar ist. Bevor Sie die Verbindung herstellen, überprüfen Sie die Version des SMB-Protokolls dieses Servers.
- Ein bestehender Ordner auf dem SMB-Server für die Datenspeicherung. Notieren Sie den Sharing-Namen. Es kann sich um anonymes Sharing (zugänglich für Gast-Konto) oder authentifiziertes Sharing (zugänglich nur für bestimmtes Benutzerkonto) handeln.

  Anmerkung: Aus Gründen der Datensicherheit wird authentifiziertes Sharing empfohlen.

- Bei authentifiziertem Sharing ist ein passwortgeschütztes Benutzerkonto erforderlich. Dieses Konto sollte Lese- und Schreibzugriff auf den Sharing-Ordner auf dem SMB-Server haben.
- Das Gerät ist mit dem Ethernet verbunden und das Netzwerk ist aktiviert.

Einrichten des Geräts

Anmerkung: Es ist wichtig, alle File-Sharing-Parameter einzugeben, bevor die File-Sharing-Option aktiviert wird, da spätere Änderungen das File Sharing deaktivieren werden. Nach der Konfiguration der Einstellungen muss das Gerät neu gestartet werden, um die Einrichtung abzuschließen. Die Änderungen der Konfiguration der Dateiübertragung werden nach dem Neustart wirksam.

1. Um die FTP/File-Share-Einstellungen zu öffnen, auf **<FTP/FS>** in der Werkzeugleiste drücken (Bildschirm 9.2).
2. In den **< FTP/File-Share Settings>** sind nur die Parameter im blauen Kasten für das File Sharing relevant (siehe Abbildung 9.2).

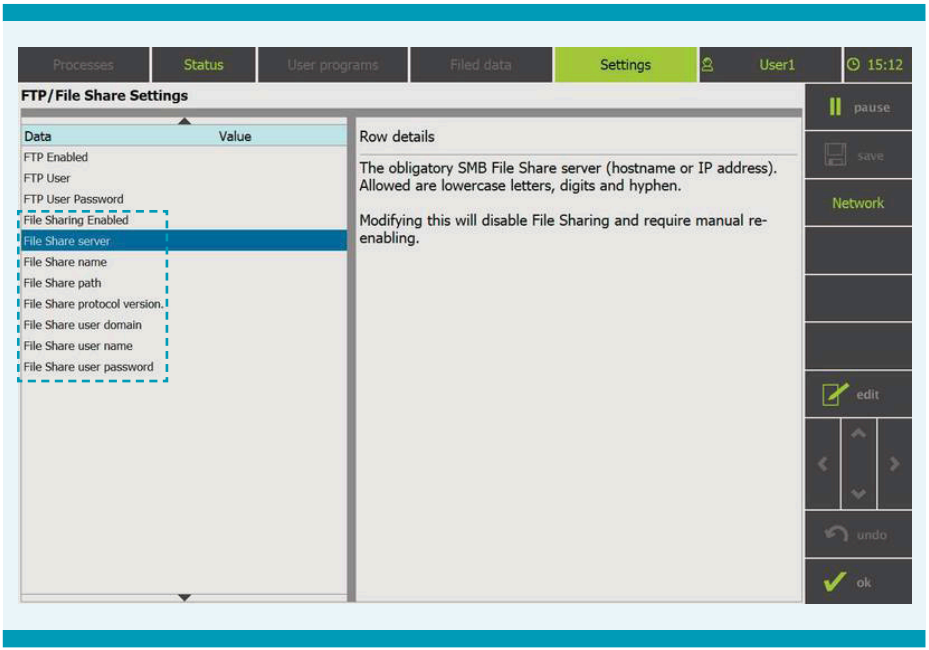


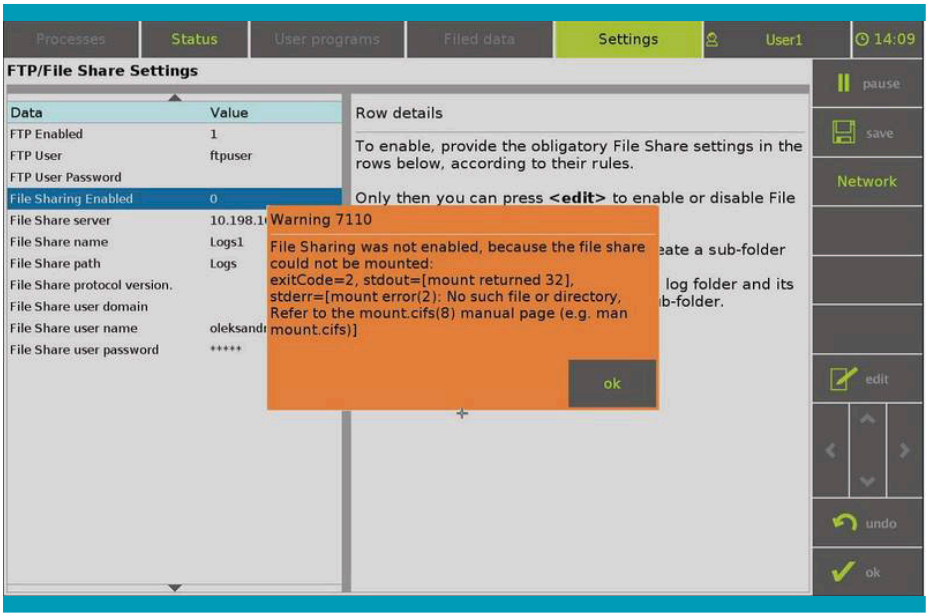
Abbildung 9.2: Parameter für das File Sharing

2. Um den Hostnamen oder die IP-Adresse des SMB-Servers einzugeben, **<File Share server>** wählen und auf **<edit>** drücken.
3. Zum Eingeben des Share-Namens **<File Share name>** wählen und auf **<edit>** drücken.
4. (Optional) Die Option **<File Share path>** wählen und auf **<edit>** drücken, um den Pfad einzugeben.
   Wenn dieser Pfad eingegeben wird, werden die vom Gerät generierten Dateien nach
   \\[File Share server]\[File Share name]\[File Share path]\ verschoben

   Wenn dieser Pfad leer ist, werden die generierten Dateien nach
   \\[File Share server]\[File Share name]\ verschoben
   Wenn der Ordner nicht gefunden wird, gibt die Software eine Warnmeldung aus (Bildschirm 9.5).

WICHTIG

Es wird empfohlen, keine Leerzeichen im File-Share-Pfad zu verwenden.



Bildschirm 9.5: Warnmeldung bei fehlgeschlagener File-Sharing-Einrichtung

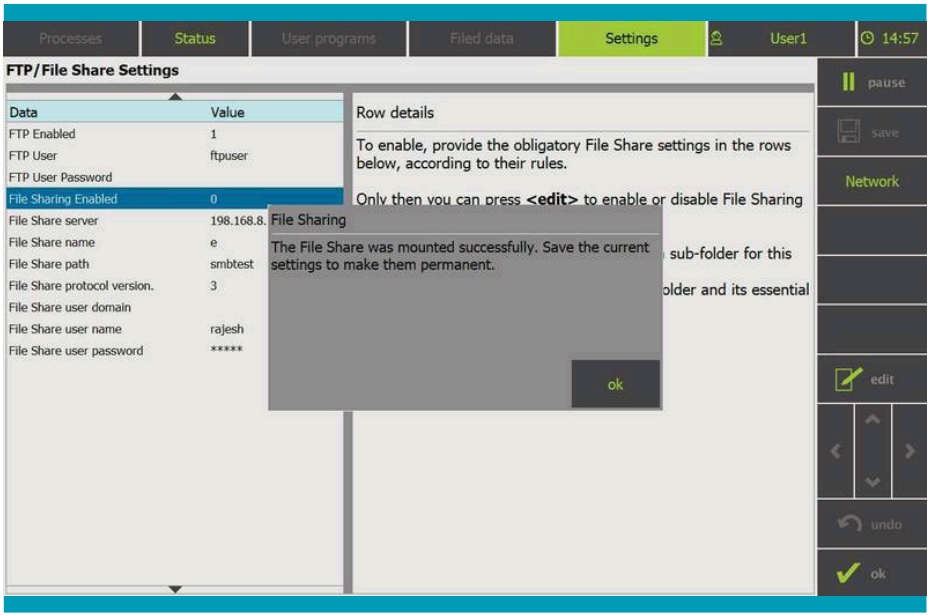
5. Zum Eingeben der Version des SMB-Protokolls **<File Share protocol version>** wählen und auf **<edit>** drücken.

6. Um die Benutzer-Domäne einzugeben, die Option **<File Share user domain>** wählen und auf **<edit>** drücken. Die Schritte für **<File Share user name>** und **<File Share user password>** wiederholen.

WICHTIG

Wenn „Gast" zur gemeinsamen Verwendung des Speicherordners verwendet wird, müssen File-Share-Benutzer-Domäne, File-Share-Benutzername und File-Share-Benutzerpasswort leer sein.

7. `**<File Sharing Enabled>** auf 1 setzen.
   Nach erfolgreicher Konfiguration wird eine entsprechende Meldung angezeigt (siehe Bildschirm 9.6).



Bildschirm 9.6: Erfolgreiche Einrichtung des File Sharing

WICHTIG

Eine Modifikation der File-Sharing-Parameter deaktiviert das File Sharing, und es muss manuell reaktiviert werden. Stellen Sie stets sicher, dass „File Sharing Enabled" aktiviert (Wert auf 1 gesetzt) ist.

9.4 Konfigurieren der Dateiübertragung über FTP

FTP ist ein Netzwerkprotokoll, das die Übertragung von Daten zwischen dem CliniMACS Prodigy (fungiert als FTP-Server) und dem Computer des Endbenutzers (fungiert als FTP-Client) über IP-(Internet-Protocol-)Verbindungen ermöglicht.

WICHTIG

- Stellen Sie sicher, dass die FTP-Verbindung nur in einem internen Netzwerk ohne Zugang zum und vom Internet verwendet wird. Die Sicherheit des Netzwerks muss vom Benutzer gewährleistet werden.
- Stellen Sie sicher, dass die Firewall-Einstellungen auf dem Client-Computer entsprechend konfiguriert sind, damit aktive oder passive FTP-Verbindungen den Datenaustausch mit dem Gerät erlauben.

Anmerkung: Über FTP zugängliche Daten des CliniMACS Prodigy sind Nur-Lese-Daten und können nur heruntergeladen werden

Um den FTP-Client mit dem Gerät zu verbinden, ist ein Login erforderlich. Das Gerät muss entsprechend der Login-Option anders konfiguriert sein. Zwei Login-Optionen werden unterstützt:

- Login-Option 1: Ein im UMS (Benutzerverwaltung) registriertes Benutzerkonto. Es ist darauf zu achten, dass die Rolle 'File management user' (Benutzer der Dateiverwaltung) diesem Konto zugewiesen ist. In diesem Fall werden die Herstellung und Beendigung der Verbindung im Audit-Trail aufgezeichnet. Weitere Informationen zu Rollen und Benutzerverwaltung finden Sie in Kapitel 10 ´Benutzerverwaltung´.
- Login-Option 2: Ein lokaler Benutzername und Passwort in den FTP/File-Sharing-Einstellungen.

9.4.1 Einrichten des Geräts

1. Zu **<FTP/File Share Settings>** gehen. Nur die Parameter im blauen Kasten sind für FTP relevant.

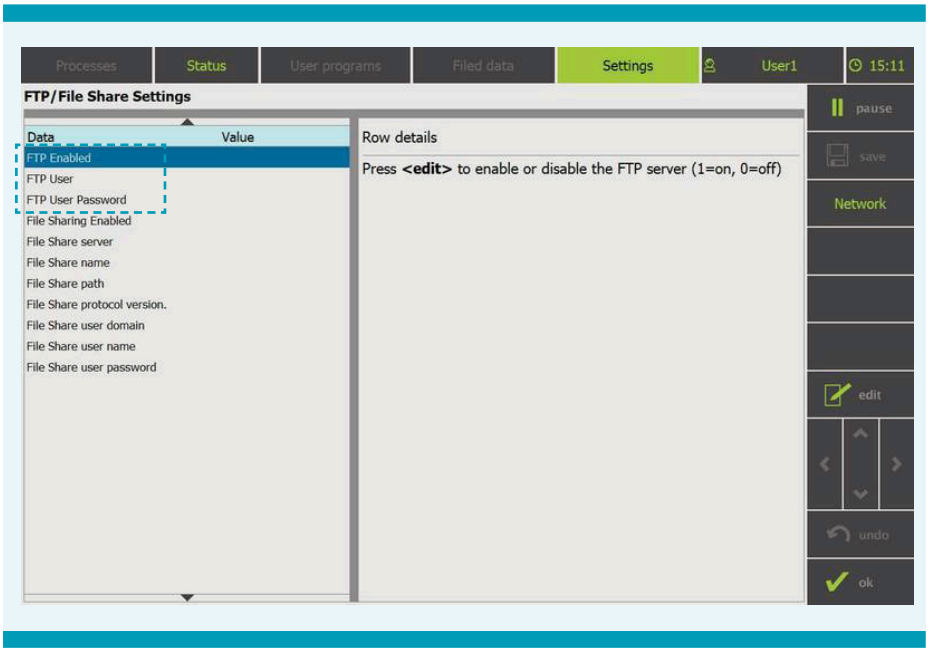


Abbildung 9.3: Parameter für das File Sharing

2. (Diesen Schritt für Login-Option 1 überspringen.) Um den Benutzernamen beim Login vom FTP-Client einzugeben, zu **<FTP User>** gehen und auf **<edit>** drücken. Der für den FTP-Client verwendete Benutzername muss nicht im Benutzerverwaltungssystem registriert sein. Der Benutzername muss mit einem Buchstaben beginnen und darf Klein- und Großbuchstaben, Ziffern und Unterstriche enthalten.

Anmerkung: Wenn <FTP User> auf 'N/A' gesetzt ist, wird die FTP-Verbindung deaktiviert.

3. (Diesen Schritt für Login-Option 1 überspringen.) Um das Passwort einzugeben, zu <FTP User Password> gehen und auf <edit> drücken. Das Passwort muss mindestens sechs Zeichen umfassen und kann aus Klein- und Großbuchstaben, Ziffern sowie den Sonderzeichen „.:+#!?= bestehen.
4. Um die FTP-Verbindung zu aktivieren, zu <FTP Enabled> gehen und den Wert durch Eingabe in das Eingabefeld auf 1 setzen.
5. Zum Speichern der Einstellungen auf <ok> in der Werkzeugleiste drücken.

9.4.2 Verbinden mit FTP-Client

Das Gerät kann mit jedem verfügbaren FTP-Client (z. B. FileZilla) verbunden werden, um nach der Konfiguration Protokolle und Protokolldateien herunterzuladen. Zur Verbindung mit dem Gerät sind folgende Angaben einzugeben:

- Die IP-Addresse des Geräts. Diese findet sich unter <Settings> ▸ <Tools> ▸ <Info> ▸ <Netzwerk-Information>.
- Port: Den Standardport 21 verwenden.
- Benutzername und Passwort:
  Für Login-Option 1: Die in der Benutzerverwaltung registrierte Konto-ID und das Passwort dazu eingeben.
  Für Login-Option 2: Den Benutzernamen und das Passwort, die wie oben in Schritt 2 und 3 beschrieben festgelegt wurden, eingeben.

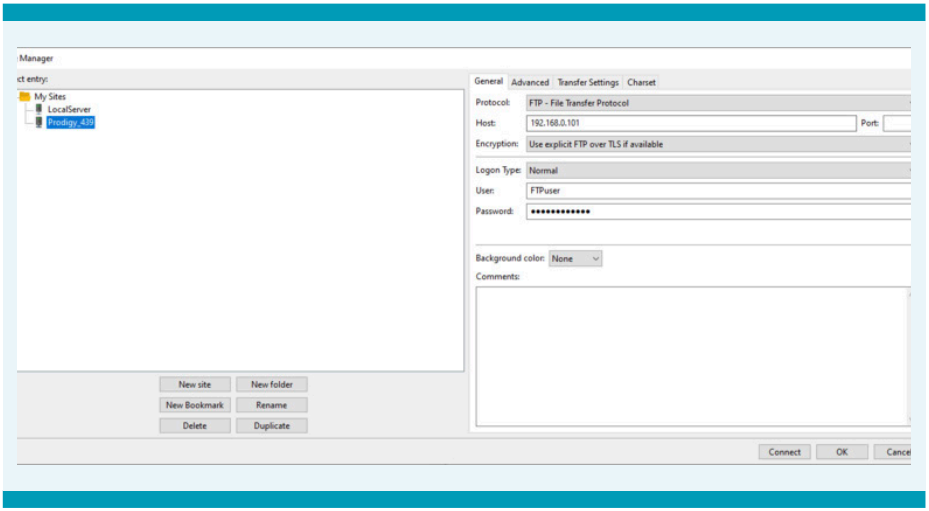


Abbildung 9.4: Beispiel für Verbindungsparameter

Anmerkung: Ein einzelner Benutzer kann immer nur eine einzige Verbindung herstellen, da der Server des Geräts keine mehrfachen Verbindungen zulässt. Wenn eine Client-Software verwendet wird, die simultane Verbindungen nutzt (z. B. FileZilla), sind die Einstellungen des Clients entsprechend dahingehend zu ändern, dass jeweils nur eine einzige Sitzung erlaubt ist. Anderenfalls kann der Inhalt nur angesehen, aber nicht heruntergeladen werden.

9.5 Verbinden mit einem E-Mail-Server

Die Software kann eine E-Mail an eine vorgegebene E-Mail-Adresse senden, wenn während eines Prozesslaufs ein Fehler auftritt und/oder Warnmeldungen ausgegeben werden. Die E-Mail enthält die Warn-/Fehlermeldungen und einen Screenshot des Geräts(siehe Abbildung 9.5). Die E-Mail-Benachrichtigung unterstützt das Simple Mail Transfer Protocol (SMTP) und das Simple Mail Transfer Protocol Secure (SMTPS).

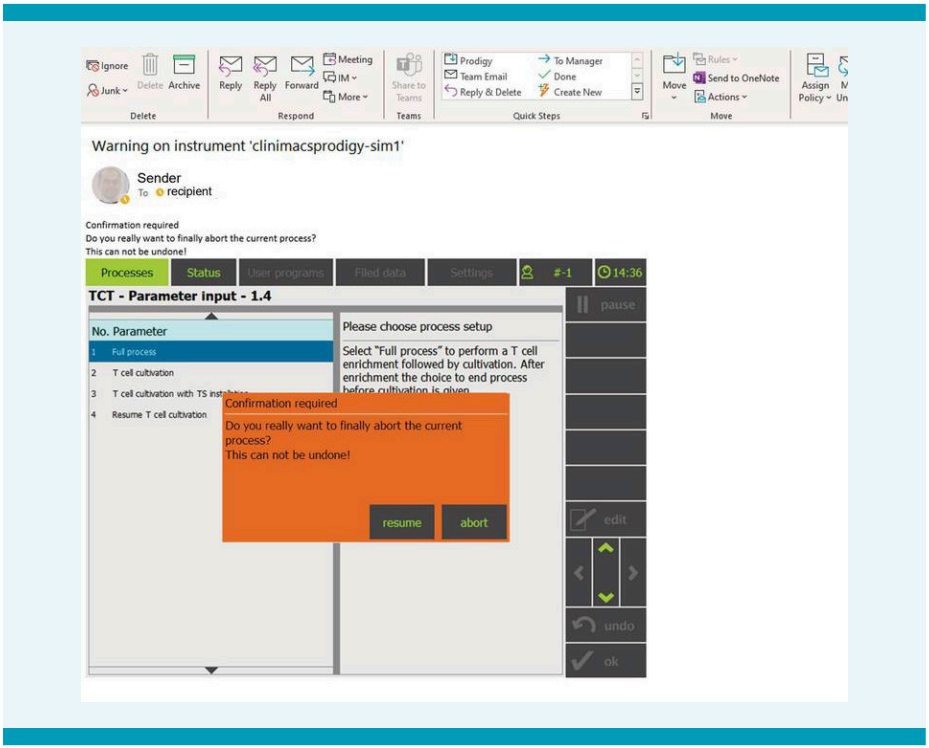


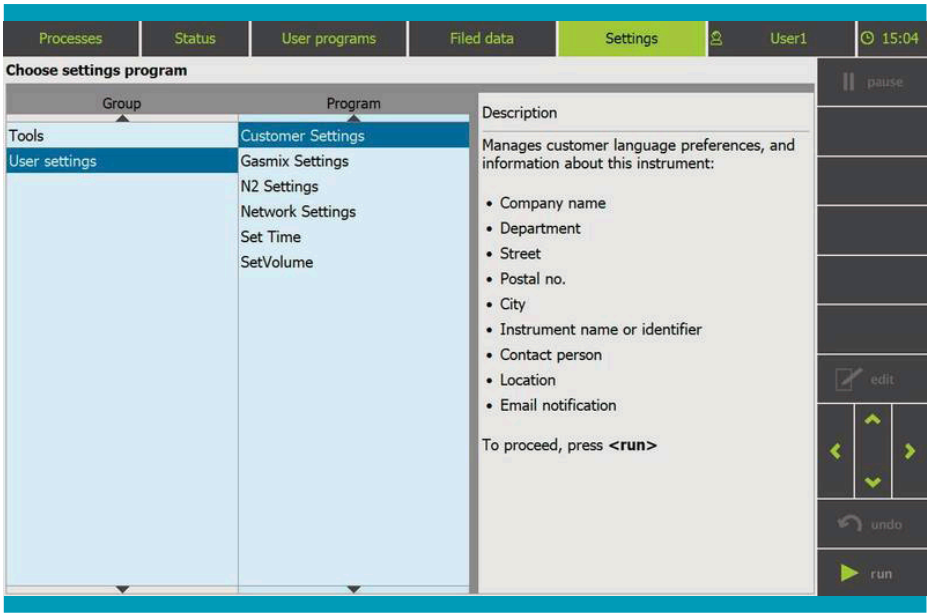
Abbildung 9.5: Beispiel-Mail

Voraussetzungen:

- Ein E-Mail-Server, der das SMTP- oder SMTPS-Protokoll unterstützt. Stellen Sie sicher, dass dieser Server erreichbar ist. Notieren Sie die IP-Adresse und den Port des Servers.
- Ein bestehender Kunden-E-Mail-Account, der zur Authentifizierung während der Einrichtung verwendet werden kann.
- Das Gerät ist mit dem Ethernet verbunden und das Netzwerk ist aktiviert.

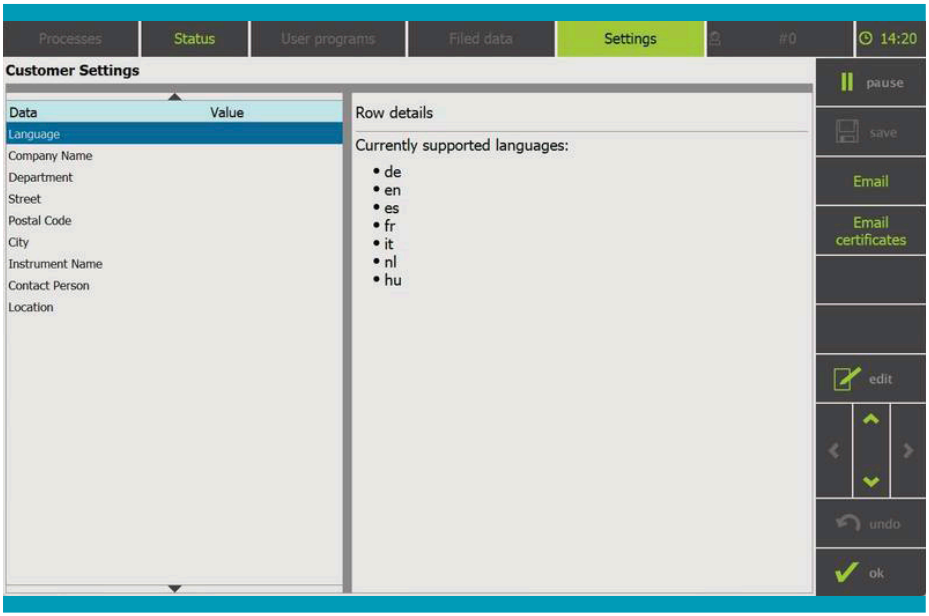
Einrichten des Geräts:

1. Um die benutzerdefinierten Einstellungen einzugeben, zu < Settings > ▸ < User settings> ▸ < Customer Settings > gehen und auf <run> drücken (siehe Bildschirm 9.7).



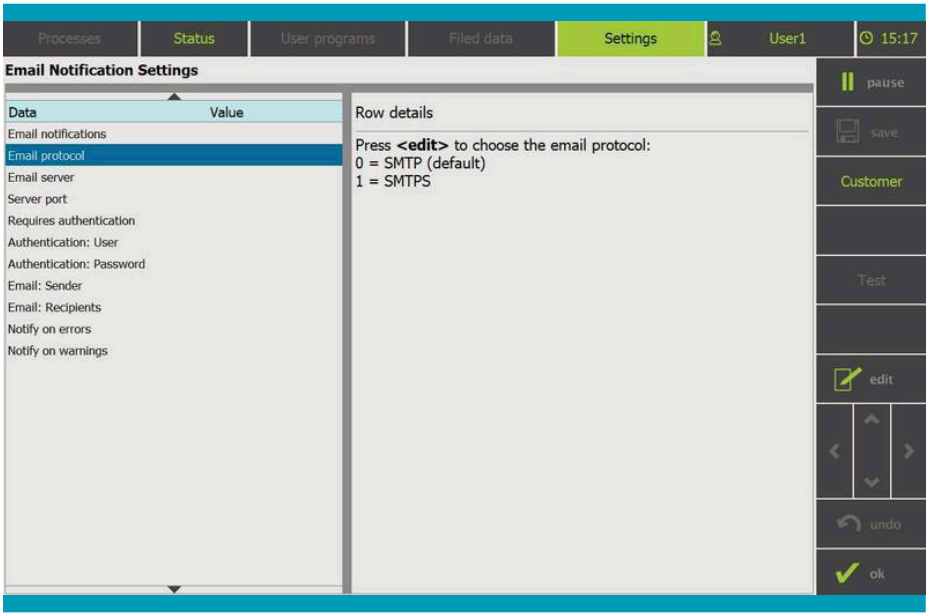
Bildschirm 9.7: Benutzerdefinierte Einstellungen starten

2. Um <Email Notification Settings> (Einstellungen für E-Mail-Benachrichtigung) einzugeben, auf <Email> in der Werkzeugleiste drücken (siehe Bildschirm 9.8).



Bildschirm 9.8: E-Mail-Einstellungen

3. Um das vom E-Mail-Server verwendete Protokoll einzugeben, zu <Email protocol> gehen und auf <edit> drücken. Standardmäßig ist SMTP(0) ausgewählt.



Bildschirm 9.9: Parameter für die E-Mail-Benachrichtigung

4. Um den Hostnamen oder die IP-Adresse des E-Mail-Servers einzugeben, zu **<Email Server>** gehen.

5. Um den im E-Mail-Server verwendeten Port einzugeben, zu **<Server port>** gehen und auf **<edit>** drücken.

Wenn der Standardport verwendet wird, braucht dieses Feld nicht bearbeitet zu werden.

Protokoll	Standardport	Alternativer Port
SMTP	25	2525, 465, 587
SMTPS	465	587 (TLS)

Tabelle 9.1: Port für E-Mail-Server

6. Die Option **<Requires authentication>** (Erfordert Authentifizierung) wählen. Wenn der E-Mail-Server eine Authentifizierung verlangt, dieses Feld auf 1 setzen und den Benutzernamen sowie das Passwort für die Authentifizierung, wie in Schritt 7 beschrieben, eingeben. Anderenfalls mit Schritt 9 fortfahren.

7. Um Benutzername und Passwort einzugeben, zu **<Authentication: User >** (Authentifizierung: Benutzer) und **<Authentication: Password>** (Authentifizierung: Passwort) gehen.**Anmerkung:** Mehrere Geräte können gemeinsam ein Authentifizierungskonto verwenden. Bitten Sie bei Bedarf Ihre IT-Abteilung um Unterstützung.

8. Um die E-Mail-Adresse des Absenders einzugeben, zu **<Email: Sender>** (E-Mail: Absender) gehen und auf **<edit>** drücken. Der **<Email: Sender>** kann derselbe wie der Authentifizierungsbenutzer sein.

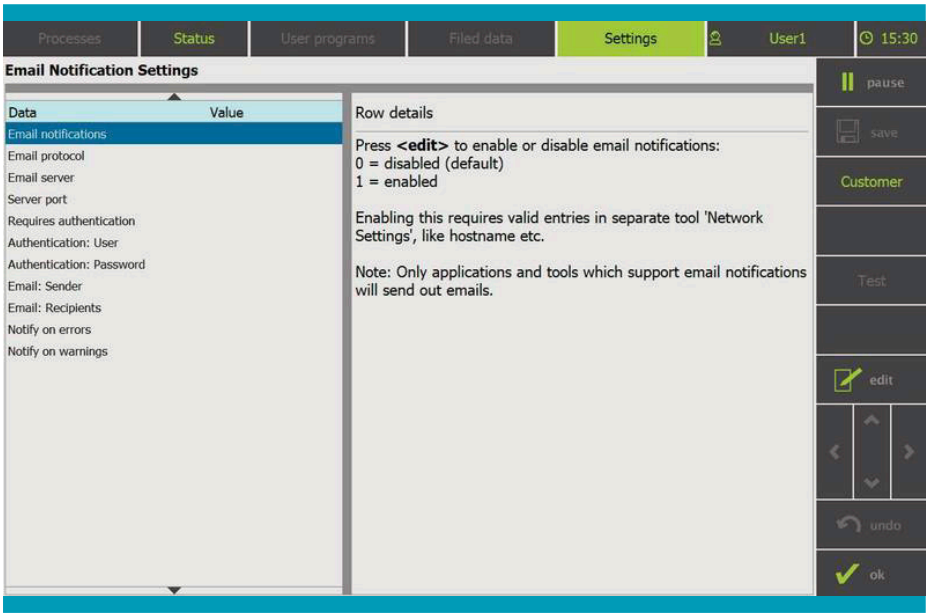
9. Um die E-Mail-Adressen der Empfänger einzugeben, zu **<Email: Recipients>** (E-Mail: Empfänger) gehen und auf **<edit>** drücken. Die Empfänger können auch eine E-Mail-Gruppen-Adresse sein.

Anmerkung: Mehrere Empfänger können, getrennt durch ein Leerzeichen, eingegeben werden.

10. Wenn Fehlermeldungen empfangen werden sollen, zu **<Notify on errors>** (Über Fehler benachrichtigen) gehen und auf **<edit>** drücken. Auf 1 setzen, um Meldungen zu aktivieren. Standardmäßig ist die Funktion **<Notify on errors>** deaktiviert (auf 0 gesetzt).

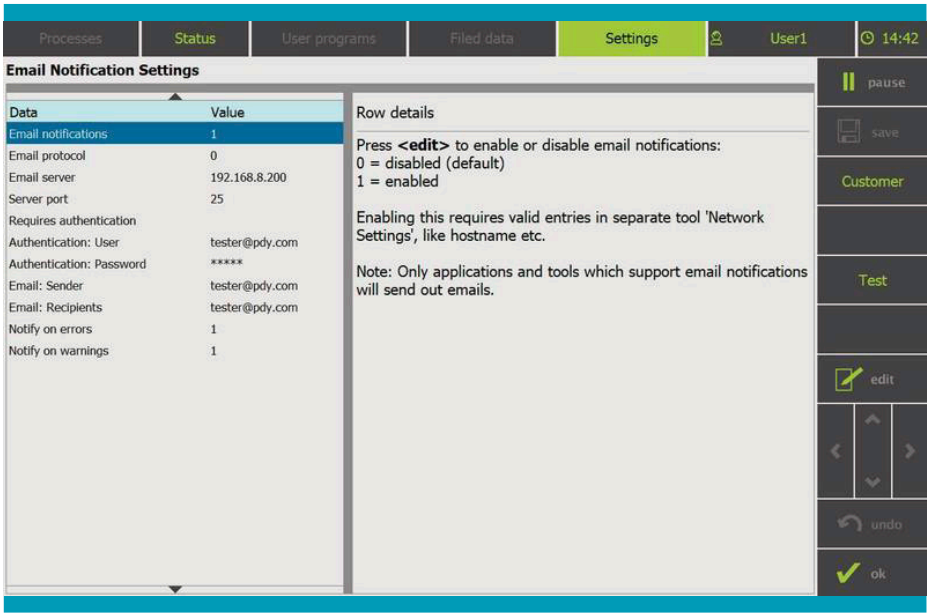
11. Wenn Warnmeldungen empfangen werden sollen, zu **<Notify on warnings>** (Über Warnmeldungen benachrichtigen) gehen und auf **<edit>** drücken. Auf 1 setzen, um Meldungen zu aktivieren. Standardmäßig ist die Funktion **<Notify on Warnings>** deaktiviert (auf 0 gesetzt).

12. Um E-Mail-Benachrichtigungen zu aktivieren, zu <Email notifications> (E-Mail-Benachrichtigungen) gehen und auf <edit> drücken (siehe Bildschirm 9.12). Auf 1 setzen, um Benachrichtigungen zu aktivieren Standardmäßig sind E-Mail-Benachrichtigungen deaktiviert (auf 0 gesetzt).



Bildschirm 9.10: Aktivieren von E-Mail-Benachrichtigungen

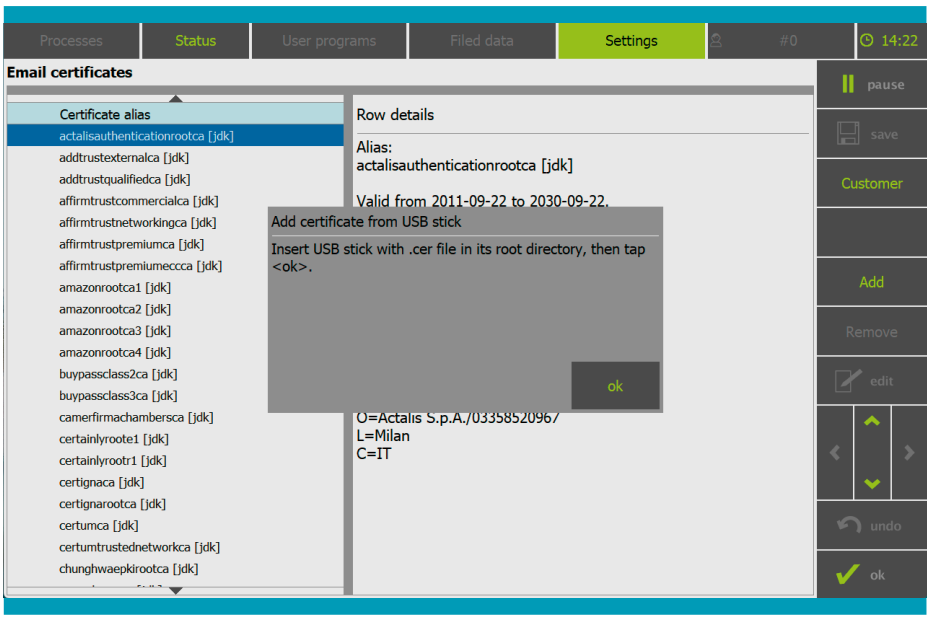
13. Wenn alle erforderlichen Informationen eingegeben sind, ist die Schaltfläche <Test> in der Werkzeugleiste aktiv. Um eine Test-E-Mail zu senden, auf <Test> in der Werkzeugleiste drücken.



Bildschirm 9.11: Senden einer Test-E-Mail

E-Mail-Zertifikate

Einige der gängigsten Zertifikate sind auf dem Gerät verfügbar. Wenn weitere Zertifikate erforderlich sind, müssen diese hochgeladen werden.



Bildschirm 9.12: Zertifikat vom USB-Stick hinzufügen

Um ein neues Zertifikat hinzuzufügen, auf < Add > drücken und den Anweisungen

auf dem Bildschirm folgen.

9.6 Aktivieren der Netzwerk-Zeitsynchronisation

NTP ist ein Netzwerkprotokoll, das die Synchronisation der Zeituhr und ein zentralisiertes Zeitmanagement ermöglicht.

Nur UMS-Benutzer mit der Administratorrolle „Administration tools user“ (Benutzer von Verwaltungstools) oder Benutzer mit der Rolle „Network setting tools user“ (Benutzer von Tools zur Netzwerkeinstellung) können auf die Netzwerkeinstellungen zugreifen. Zur Aktivierung der NTP-Funktionalität auf dem Gerät ist wie folgt vorzugehen:

1. Zu **<Settings>** ▸ **<User settings>** ▸ **<Network Settings>** gehen und auf **<run>** drücken. Die Netzwerkkonfiguration wird angezeigt. Die Parameter im blauen Kasten sind für die Netzwerk-Zeitsynchronisation relevant (siehe Abbildung 9.6).

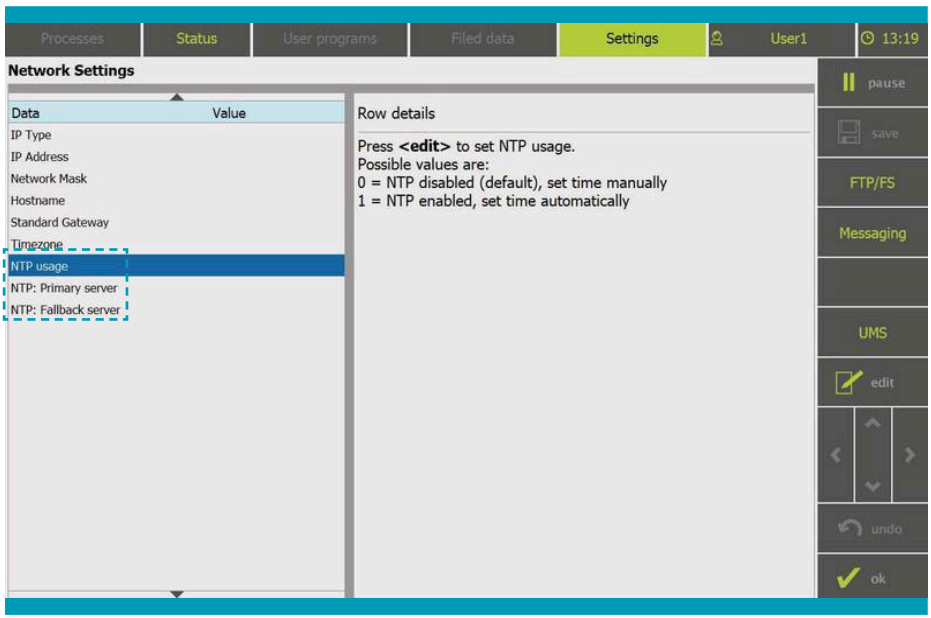


Abbildung 9.6: NTP-Einstellungen

2. Um NTP und die automatische Zeiteinstellung zu aktivieren, auf **<NTP usage>** (NTP-Nutzung) drücken und den Wert auf 1 setzen, dann im Eingabefeld auf **<ok>** drücken.

3. Um Hostname/IP-Adresse einzugeben, auf **<NTP: Primary server>** (NTP: Primär-Server) oder **<NTP: Fallback server>** (NTP: Ersatzserver) und anschließend auf **<edit>** drücken. Zur Bestätigung der Eingabe auf **<ok>** drücken.

4. Auf **<save>** drücken und bestätigen, dass diese Änderungen akzeptiert und gespeichert werden sollen. Die NTP-Server-Einstellungen sind aktiviert.
5. Das System neu starten (siehe Abschnitt 8.7 ´Ausschalten´).

10 Benutzerverwaltung

10.1 Allgemeine Informationen

Das Benutzerverwaltungssystem in der Software unterstützt die Benutzerauthentifizierung und die rollenbasierte Zugangskontrolle, um die Vorschriften von 21 CFR Part 11 einzuhalten.

- Benutzerauthentifizierung: Benutzername (auch als Konto-ID bezeichnet) und Passwort sind erforderlich, um sich am Gerät einzuloggen und es verwenden zu können. Sowohl die lokale Benutzerverwaltung als auch die LDAP-Authentifizierung werden unterstützt.
- Rollenbasierte Zugangskontrolle: Benutzer mit unterschiedlichen Rollen haben unterschiedliche Zugangsrechte. In der rollenbasierten Zugangskontrolle sind drei Begriffe definiert: Rechte, Rollen und Konten.

Rechte

Rechte stellen die minimal zuweisbare Einheit von Benutzeraktionen dar. Die Rechte werden durch die Software definiert, und der Benutzer kann nur die bestehenden Rechte gruppieren. Eine Übersicht der verschiedenen Rechte in der Software finden Sie in Table A.1 im Anhang.

Rollen

Rollen entsprechen Arbeitsfunktionen oder Verantwortlichkeiten innerhalb eines Unternehmens. Einer Rolle kann eine Sammlung von Rechten zugewiesen werden. Die Software stellt Standardrollen zur Verfügung. Eine Auflistung der wichtigsten Standardrollen finden Sie in Tabelle 10.1. Die Software unterstützt kundenspezifische Rollen.

Konten

Konten entsprechen einzelnen Benutzern. In einer GMP-Umgebung muss eine Eins-zu-Eins-Beziehung zwischen einer Person und einer Konto-ID bestehen. Bei der Installation wird ein Administratorkonto mit allen Rollen erstellt. Dieses ermöglicht dem betreffenden Benutzer, nach Bedarf neue Rollen und Konten anzulegen.

Rolle	Werkzeuge/Rechte
Application x.x operator (Bediener von Anwendung x.x)	Erlaubnis, diese Anwendung mit Versionsnummer x.x durchzuführen
ATS user (ATS-Benutzer)	Zugriff auf Audit Trails, einschließlich Anzeigen, Exportieren und Löschen
Administration tools user (Benutzer von Verwaltungstools)	Zugriff auf Tools zur Verwaltung des Geräts. Wird für Administratoren empfohlen
Common tools user (Benutzer von allgemeinen Tools)	Zugriff auf allgemeine Tools: info, license, shutdown und user settings Wird für alle Benutzer empfohlen
File management user (Benutzer der Dateiverwaltung)	Zugriff auf das Tool Backup Filed Data und das Tool Custom Files. Ermöglicht Zugriff auf Protokolldateien über FTP
Gas mix tool v1.0 Operator (Bediener des Gasgemisch-Tools v1.0)	Bedienerzugriff auf das Gasmisch-Tool
Injected programs (Injizierte Programme)	Erlaubnis zur Ausführung von injizierten Programmen
N_2 settings tools user (Benutzer des N_2-Einstellungstools)	Zugriff auf das Tool N_2 settings (N_2-Einstellungen)
Set time user (Benutzer mit Zeit-Einstellberechtigung)	Ermöglicht das Einstellen der Uhrzeit
Support tools user (Benutzer von unterstützenden Tools)	Zugriff auf die Tools Chamber in, Chamber out, Sealer und Instrument Check
UM Administrator (BM Administrator)	Zugriff auf die Benutzerverwaltung zum Verwalten der Konten
UM user	Definierter Bediener, der die Benutzeranwendung starten und ausführen soll

Tabelle 10.1: Übersicht über Standardrollen

Das folgende Beispiel zeigt eine konventionelle UMS-Einrichtung:

- Ein Administrator verwaltet Konten und das Gerät. Die Administratorrolle ermöglicht normalerweise das Einrichten und Ändern von Konten sowie den

Zugriff auf die Dateiverwaltung und erweiterte Tools für Geräteeinstellungen.

- Ein Bediener startet und führt Anwendungen auf dem Gerät aus. Das Bedienerkonto wird eingerichtet, um die Ausführung einer Reihe von bestimmten Anwendungen und Tools basierend auf kundenspezifischen Benutzerverwaltungsentscheidungen zur Unterstützung und Fehlerbehebung zu erlauben. Es kann mehr als ein kundendefinierter Benutzertyp konfiguriert sein, und jedem Benutzer können eine oder mehrere Rollen zugewiesen sein.

WICHTIG

Einem Bediener muss die Rolle „UM User“ zugewiesen werden. Einem Administrator muss die Rolle „UM Administrator“ zugewiesen werden.

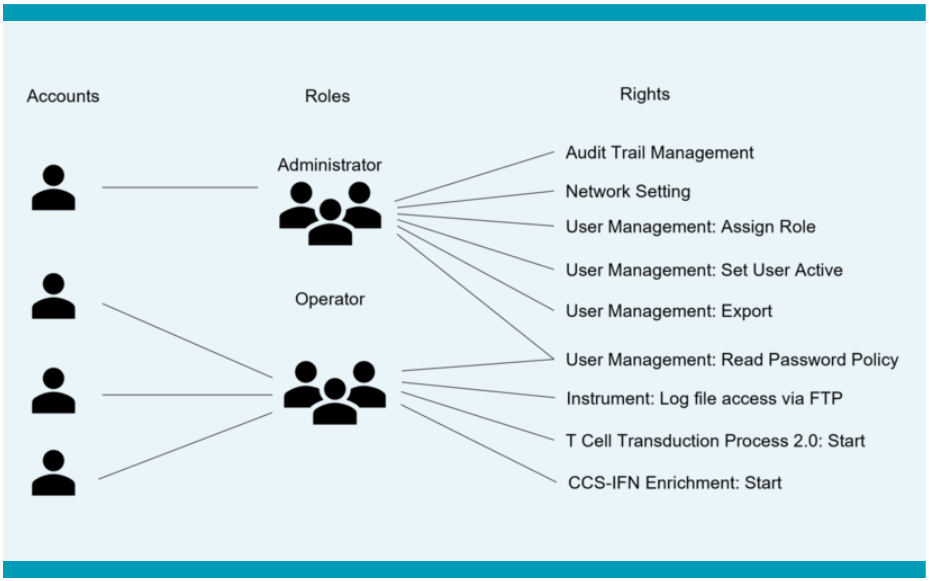


Abbildung 10.1: Beispiel für Verbindungsparameter

⚠ VORSICHT

Gefahr eines Prozessfehlers durch fehlgeschlagenes Login. Wenn kein Login mehr möglich ist, besteht die Gefahr eines Prozessfehlers. Um eine solche Situation zu vermeiden, müssen entsprechende Benutzer- und Administratorkonten mit eigenen Passwörtern erstellt werden, bevor Anwendungen auf dem Gerät gestartet werden. Für den Fall, dass ein Login in das Gerät nicht mehr möglich ist, kontaktieren Sie den Miltenyi Biotec Technical Support.

WICHTIG

- Es wird dringend empfohlen, für Notfälle einen Notfallzugriff einzurichten. Dies kann ein zusätzliches Administratorkonto zur Verwendung im Notfall sein. Die

Zugangsdaten des Notfallkontos sollten an einem sicheren Ort verwahrt werden und nur bestimmten Personen zugänglich sein.

- Das Authentifizierungsverfahren sollte beschrieben und innerhalb des Qualitätsmanagementsystems der Einrichtung implementiert werden. Alle Benutzer und Administratoren müssen entsprechend geschult werden.
- Wenn die LDAP-Verbindung fehlschlägt, verwenden Sie ein lokales Benutzerkonto für den Zugang zum Gerät.

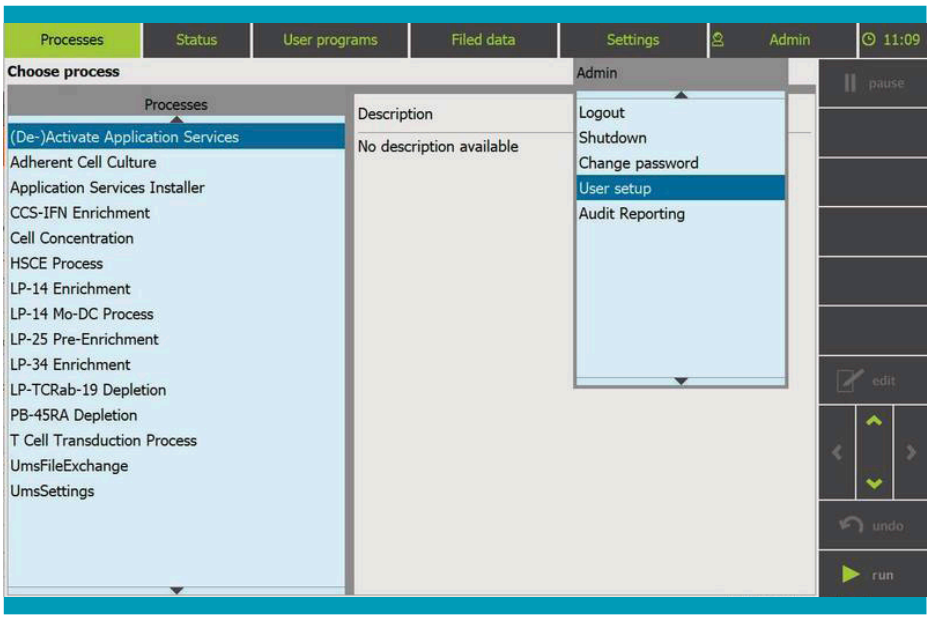
10.2 Verwalten von Rollen und Konten

WICHTIG

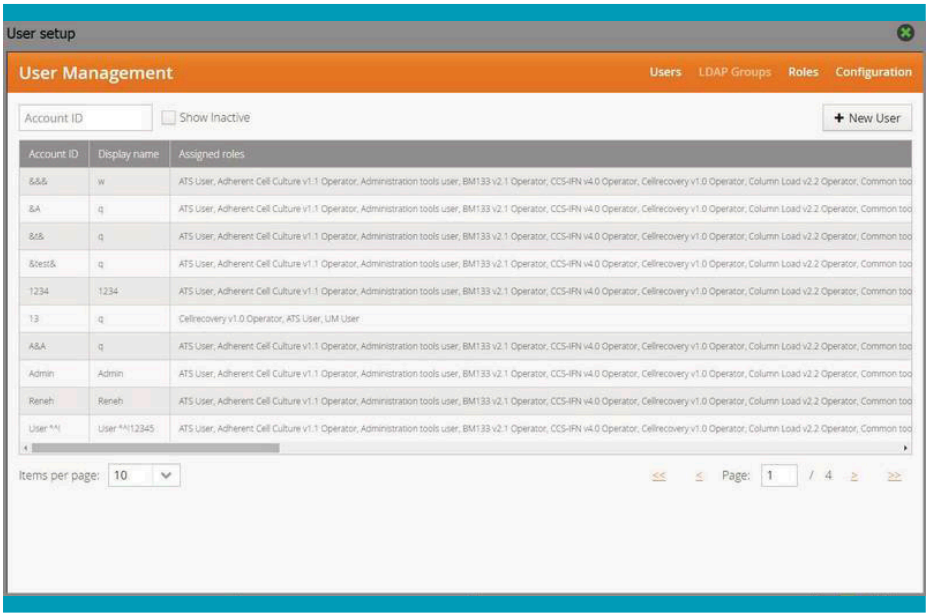
Ein Benutzer muss die Rolle „UM Administrator“ haben, um das Benutzerverwaltungssystem zu konfigurieren.

10.2.1 Zugriff auf die Benutzerverwaltung

Um das Benutzerverwaltungssystem aufzurufen, zu (Schnellzugriffsmenü) gehen und auf <User setup> drücken. Die Seite „User Management“ (Benutzerverwaltung) wird angezeigt (Bildschirm 10.2). Die Benutzerverwaltung umfasst vier Seiten: <Users> (Benutzer), <LDAP Groups> (LDAP-Gruppen), < Roles> (Rollen) und <Configuration> (Konfiguration). Als erste Seite wird standardmäßig <Users> angezeigt.



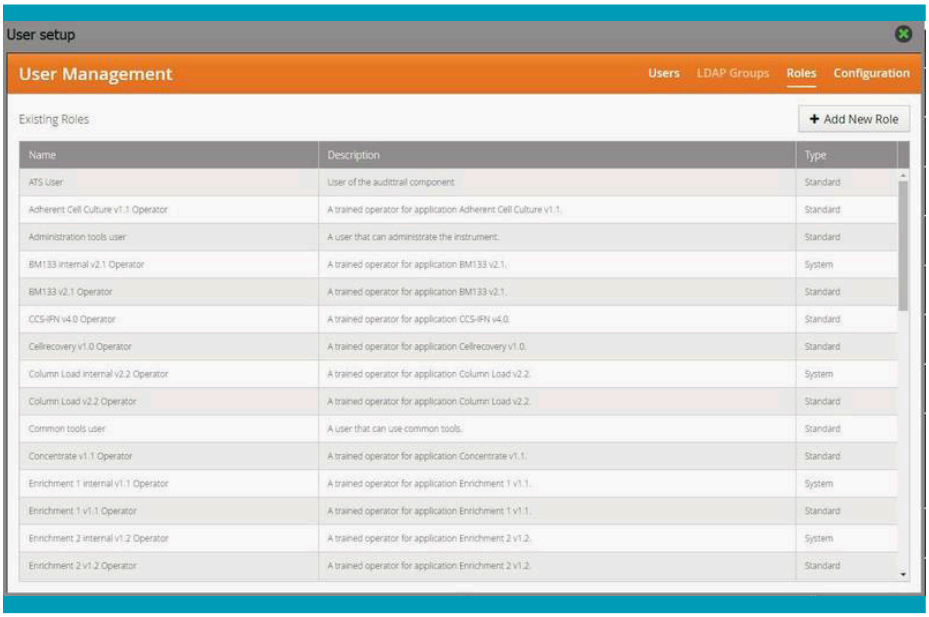
Bildschirm 10.1: Wählen der Option „User setup“



Bildschirm 10.2: Menü „User Management“

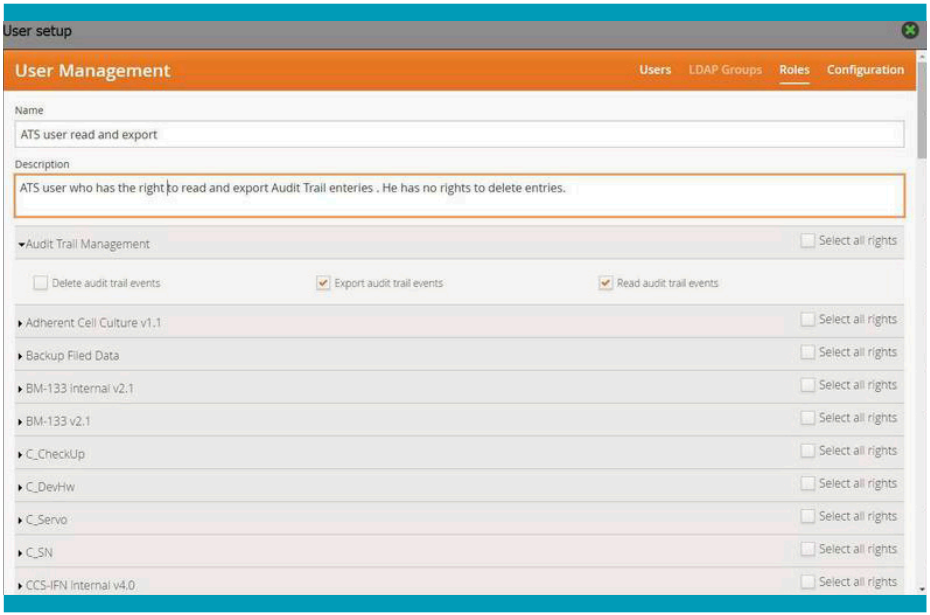
10.2.2 Erstellen einer neuen Rolle

1. Auf <Roles> (Rollen) in <User Management> drücken. Eine Liste der bestehenden Rollen wird angezeigt (Bildschirm 10.3).



Bildschirm 10.3: Definierte Rollen in der Benutzerverwaltung

2. Auf <+Add New Role> (Neue Rolle hinzufügen) drücken (Bildschirm 10.3). Eine Seite zur Definition einer neuen Rolle wird angezeigt (siehe Bildschirm 10.4).



Bildschirm 10.4: Erstellen einer neuen Rolle

3. Den Namen und die Beschreibung der Rolle eingeben. Die gewünschten Rechte für diese Rolle markieren.
4. Unten auf der Seite auf <save> (Speichern) drücken. Die neu hinzugefügte Rolle wird in der Liste der bestehenden Rollen angezeigt und kann einem Benutzer zugewiesen werden.

10.2.3 Ändern der Rechte von Rollen

1. Die Rolle in der Liste der bestehenden Rollen suchen und auswählen (siehe Bildschirm 10.3)
2. Die gewünschten Rechte selektieren oder deselektieren.

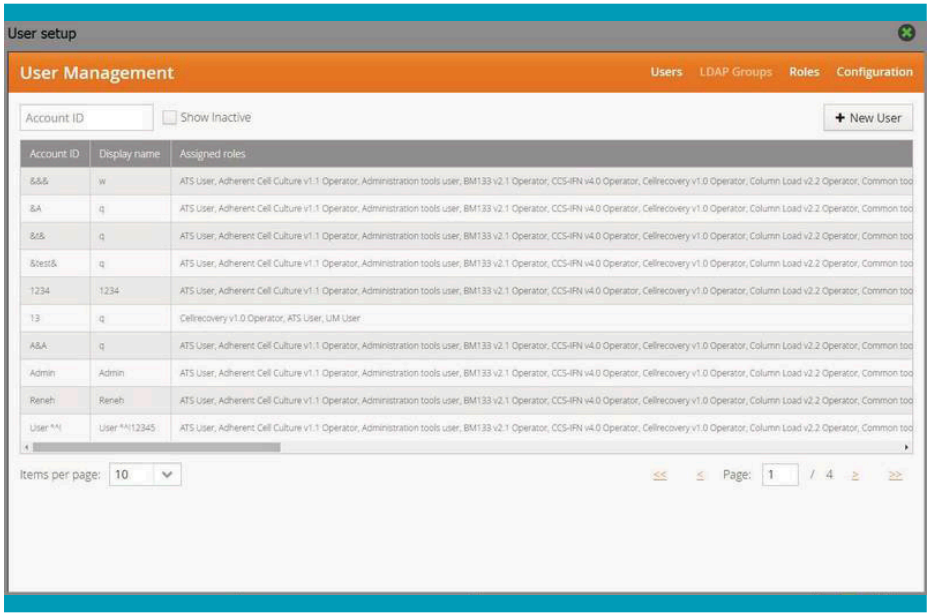
3. Nach unten scrollen und auf <save> drücken.

10.2.4 Hinzufügen eines lokalen Benutzers

WICHTIG

- Ein Benutzer muss die Rolle „UM Administrator“ haben, um ein neues Konto erstellen zu können.
- In einer GMP-Umgebung müssen natürlich echte Namen oder Synonyme verwendet werden, die klar unterscheidbar und erkennbar sind.

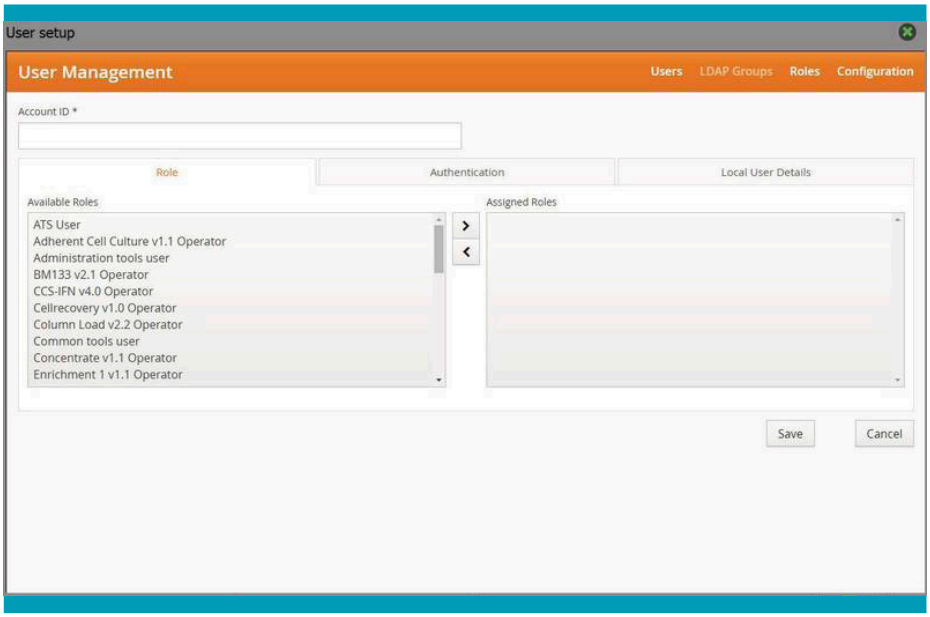
1. In der Benutzerverwaltung das Menü <Users> wählen.
2. Auf <+New User> (Neuer Benutzer) drücken. Die Seite zum Hinzufügen eines neuen Benutzers wird angezeigt (Bildschirm 10.5).



Bildschirm 10.5: Menü „New user“

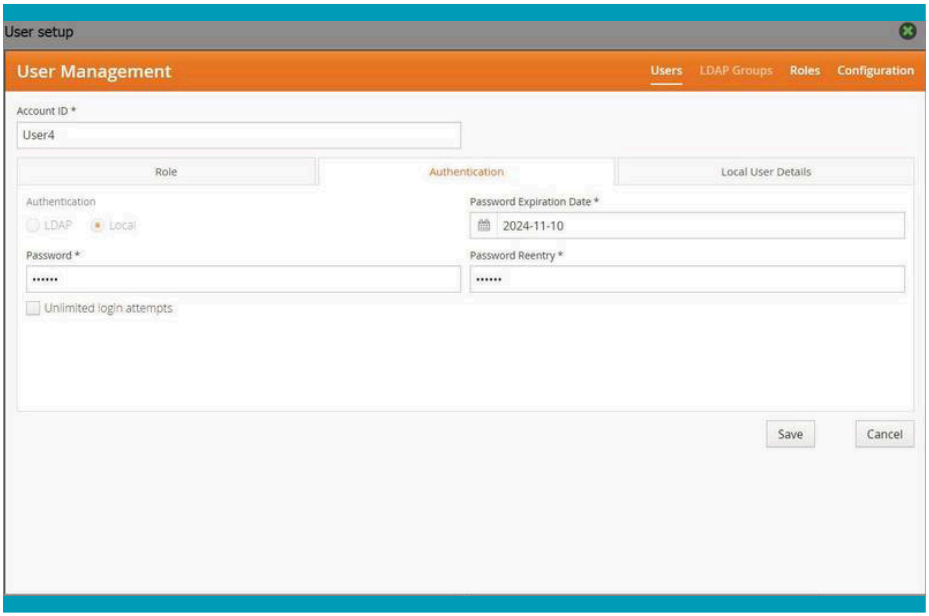
3. Die Konto-ID eingeben (Bildschirm 10.6). Diese Konto-ID muss eindeutig sein und eine Eins-zu-Eins-Beziehung zu einem Endbenutzer haben. Die Konto-ID entspricht dem Benutzernamen beim Login. Wenn das Active Directory konfiguriert ist, überprüft die Software, ob diese ID im AD-Server registriert ist. Wenn die ID nicht gefunden wird, wird ein lokales Konto erstellt. Wenn die ID gefunden wird, wird standardmäßig das AD-Konto verwendet. Um ein LDAP-Konto in ein lokales Konto zu ändern, Schritt 5 befolgen.
4. Um diesem Konto die entsprechenden Rollen zuzuweisen, den Eintrag in <Available Roles> (Verfügbare Rollen) auf der Registerkarte <Role> (Rolle)

wählen und auf [›] drücken (Bildschirm 10.6). Um eine zugewiesene Rolle von diesem Konto zu entfernen, den Eintrag in **<Assigned Roles>** (Zugewiesene Rollen) wählen und auf [‹] drücken.



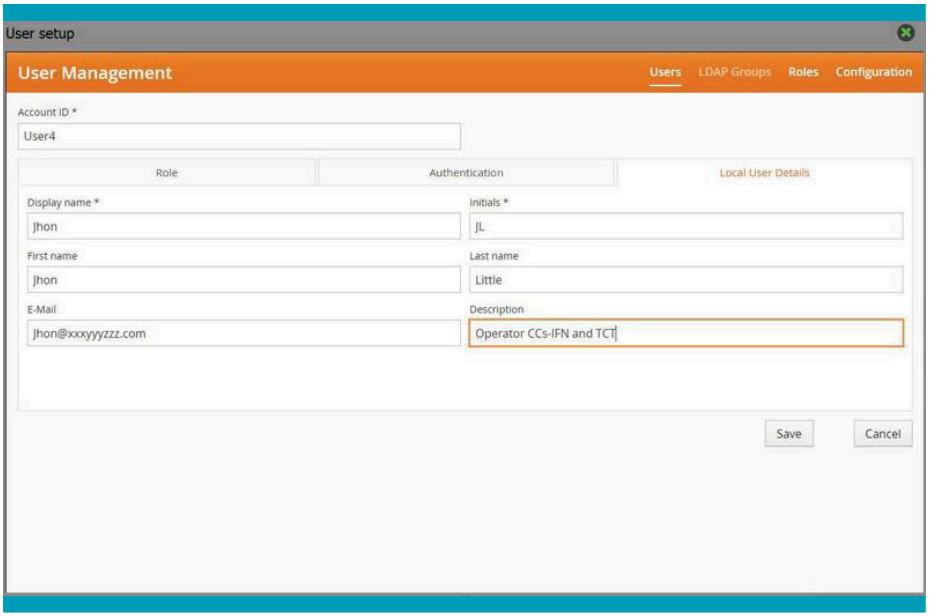
Bildschirm 10.6: Benutzerkonfigurationsseite

5. Wenn LDAP konfiguriert ist und die Konto-ID auf dem AD-Server gefunden wird, kann der Benutzer zwischen der Authentifizierung über den AD-Server oder die lokale Datenbank wählen. Für einen lokalen Benutzer das Passwort eingeben und das Ablaufdatum entsprechend den Passwortrichtlinien festlegen (siehe Abschnitt 10.3 „Konfigurieren der Passwortrichtlinien“).



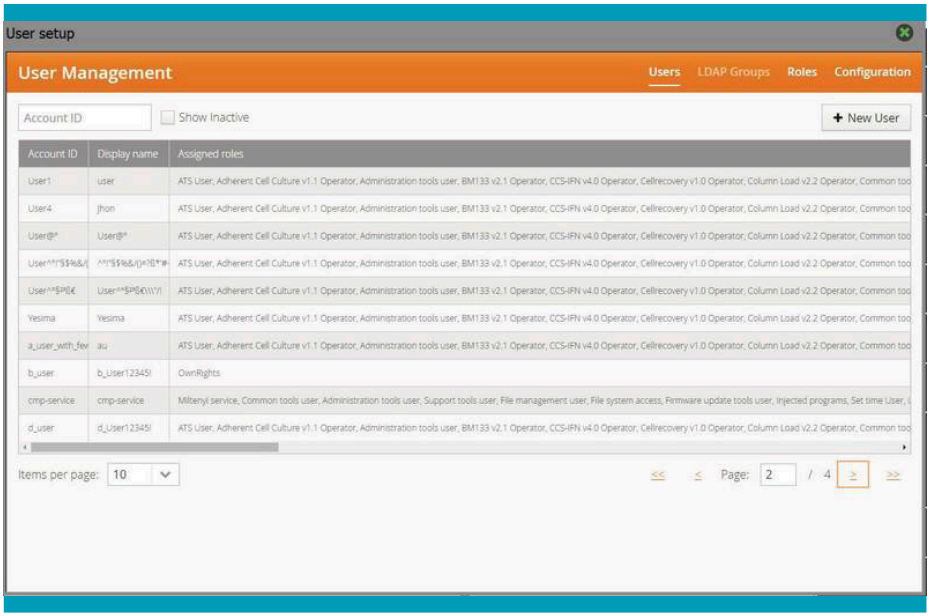
Bildschirm 10.7: Eingeben des Passworts für den neuen Benutzer

6. Auf der Registerkarte <Local User Details> (Details des lokalen Benutzers) genauere Informationen zu diesem Konto einstellen.



Bildschirm 10.8: Eingeben der Details zum lokalen Benutzer

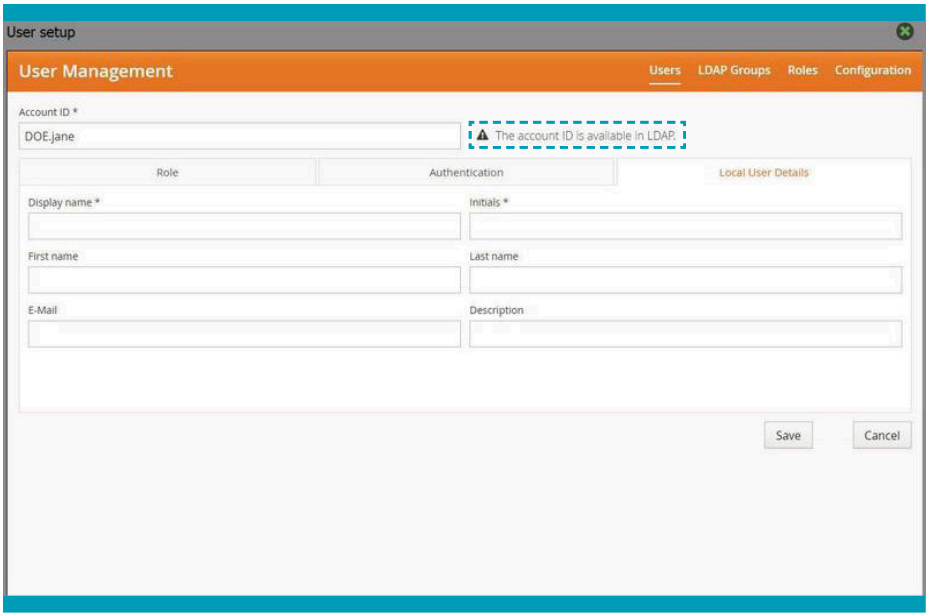
7. Auf <save> drücken. Das neu hinzugefügte Konto erscheint in der Kontoliste (Bildschirm 10.9).



Bildschirm 10.9: Bestätigung eines neu hinzugefügten Benutzers

10.2.5 Hinzufügen von LDAP-Benutzern

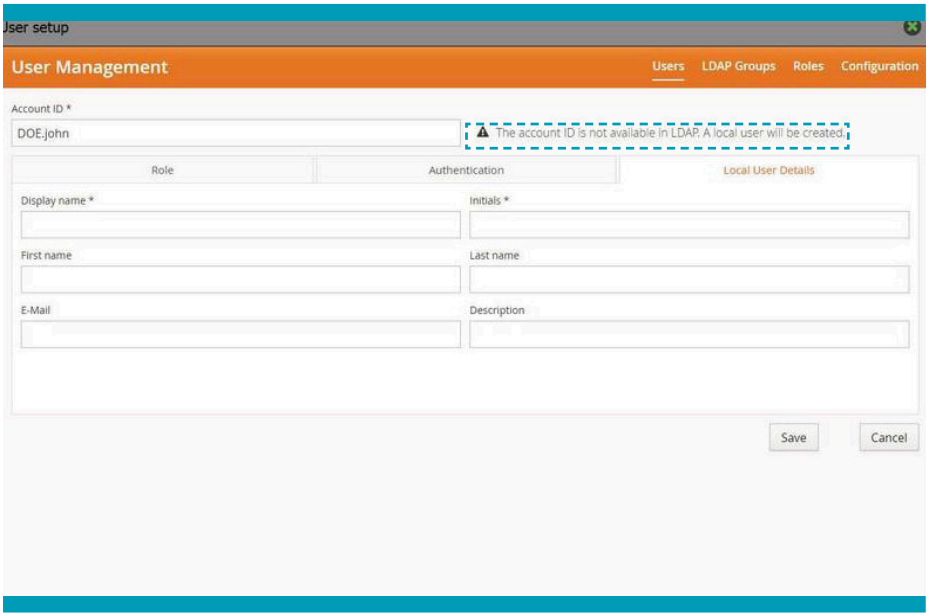
1. Zu <Users> in <User Management> gehen.
2. Auf <+New User> (Neuer Benutzer) drücken.
3. Die LDAP-Konto-ID eingeben. Die Software überprüft, ob diese ID im AD-Server registriert ist. Wenn der Benutzer bereits existiert, werden weitere Informationen mittels Attribute Mapping angezeigt (siehe Bildschirm 10.10). Wenn der Benutzer nicht in AD registriert ist, wird ein neuer lokaler Benutzer angelegt (siehe Bildschirm 10.11).



Bildschirm 10.10: User Management mit registriertem LDAP-Benutzer

4. Um Rollen zuzuweisen, auf <Role> drücken und die gewünschten Rollen wählen.

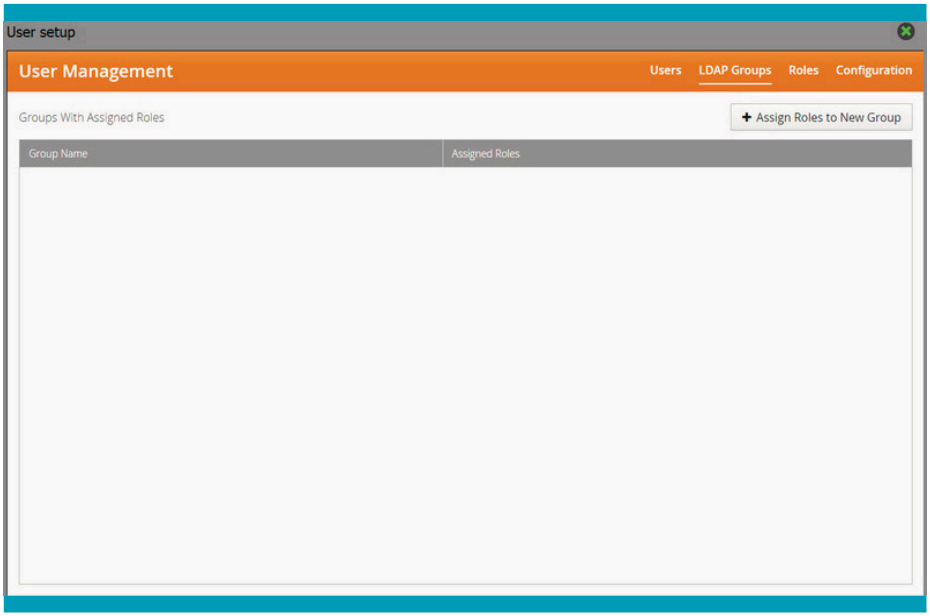
5. Auf <save> (Speichern) drücken. Der Benutzer kann die LDAP-Konto-ID und das zugehörige Passwort verwenden, um sich im System einzuloggen.



Bildschirm 10.11: User Management mit nicht registriertem LDAP-Benutzer

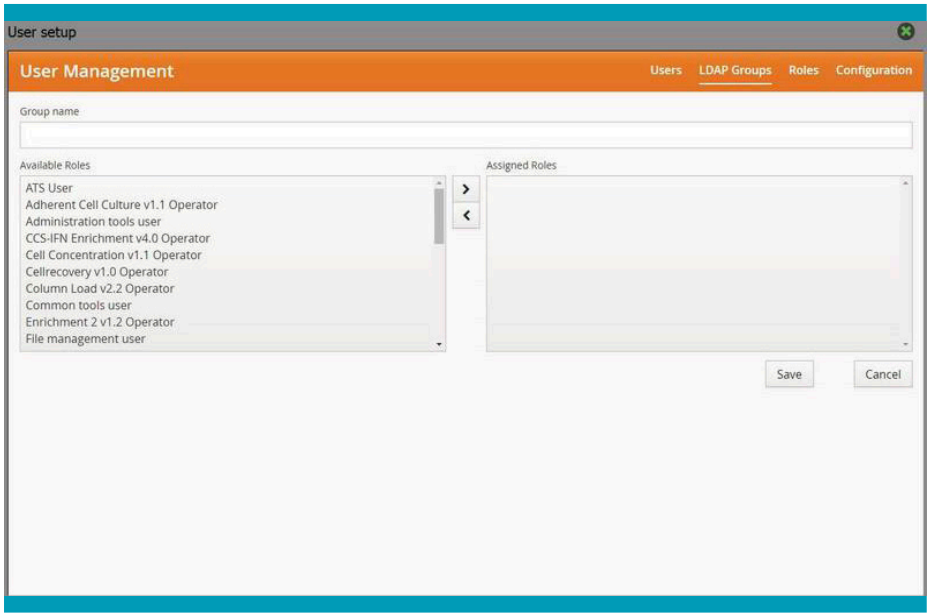
10.2.6 Hinzufügen von LDAP-Gruppen

1. <LDAP Groups> (LDAP-Gruppen) in der Menüleiste wählen und auf <+ Assign Roles to New Group> (Rollen zu neuer Gruppe zuweisen) drücken.



Bildschirm 10.12: Menü User Management und Schritt zum Hinzufügen von LDAP-Gruppen

2. Einen Gruppennamen eingeben (siehe Bildschirm 10.13). Das System überprüft automatisch, ob diese Gruppe in LDAP existiert.
3. Um Rollen zu dieser Gruppe zuzuweisen, die Rollen in <Available Roles> auswählen und auf ▷ drücken. Um eine zugewiesene Rolle von dieser Gruppe zu entfernen, den Eintrag in <Assigned Roles> wählen und auf ◁ drücken.
4. Auf <save> (Speichern) drücken.



Bildschirm 10.13: User Management mit Menü LDAP Groups

WICHTIG

Stellen Sie sicher, dass Sie den korrekten „UM Administrator" oder „UM User" hinzufügen, um ein ordnungsgemäßes Login zu gewährleisten.

10.2.7 Ändern der zugewiesenen Rollen eines Benutzers oder einer LDAP-Gruppe

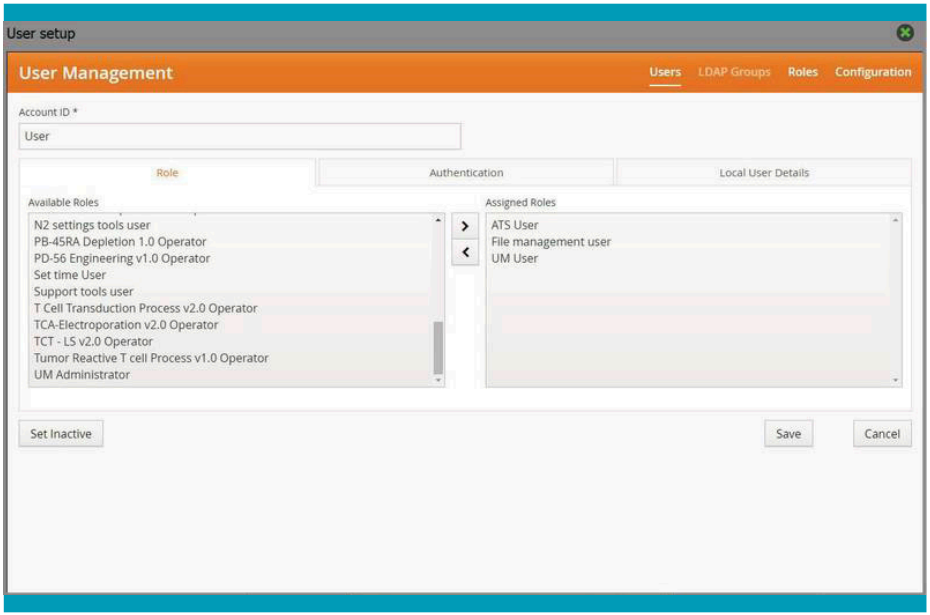
1. Den Benutzer in der Benutzerliste auf der Seite Users wählen (Bildschirm 10.2) und die entsprechende Registerkarte öffnen. Für LDAP-Gruppe die gewünschte Gruppe auf der Seite LDAP Groups wählen (Bildschirm 10.12).
2. Um dem Benutzer zusätzliche Rollen zuzuweisen, den Eintrag in **<Available Roles>** auf der Registerkarte **<Role>** wählen und auf ▷ drücken. Um zugewiesene Rollen von diesem Konto zu entfernen, den Eintrag in **<Assigned Roles>** wählen und auf ◁ drücken.
3. Auf **<Save>** unten auf der Registerkarte **<Role>** drücken.

10.2.8 Deaktivieren lokaler Benutzer

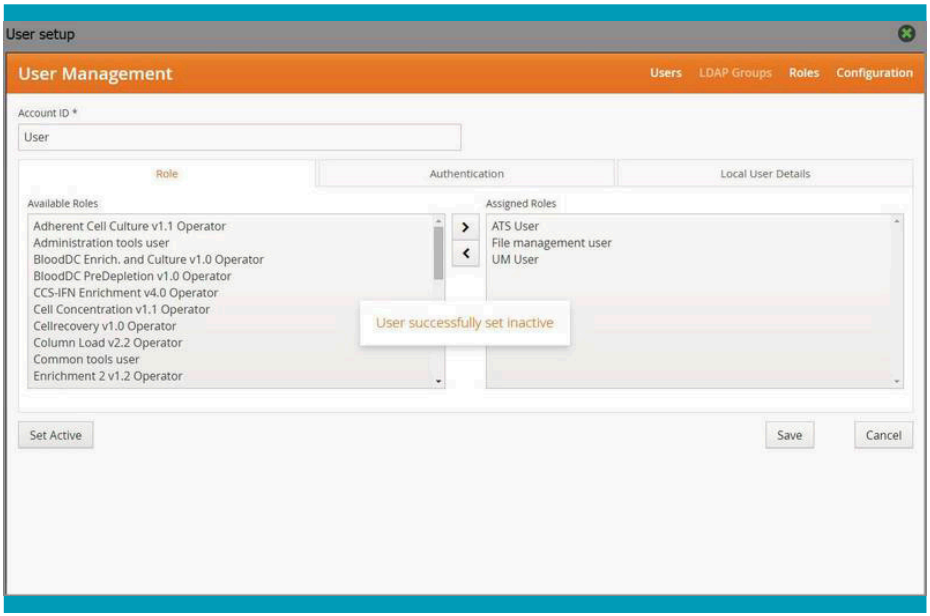
Anmerkung: Ein lokaler Benutzer kann nicht gelöscht, sondern nur deaktiviert werden.

1. Den lokalen Benutzer aus der Benutzerliste wählen (Bildschirm 10.9). Die Benutzerkonfigurationsseite wird angezeigt.

2. Auf <Set Inactive> (Inaktiv setzen) unten auf der Benutzerkonfigurationsseite drücken (Bildschirm 10.14).

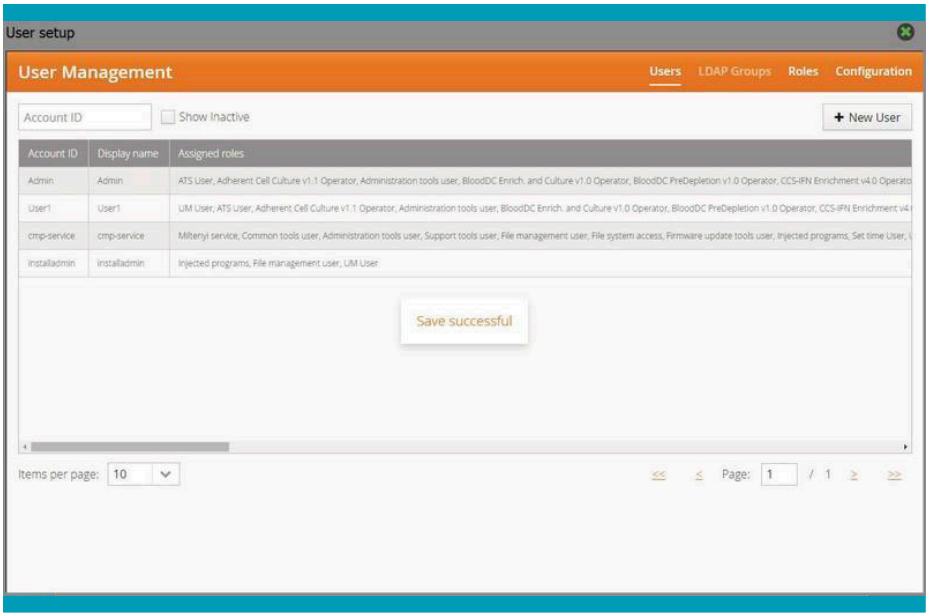


Bildschirm 10.14: Deaktivieren eines lokalen Benutzers



Bildschirm 10.15: Erfolgreich deaktivierter Benutzer

3. Auf <Save> unten auf der Seite drücken, um zur Benutzerliste zurückzukehren.

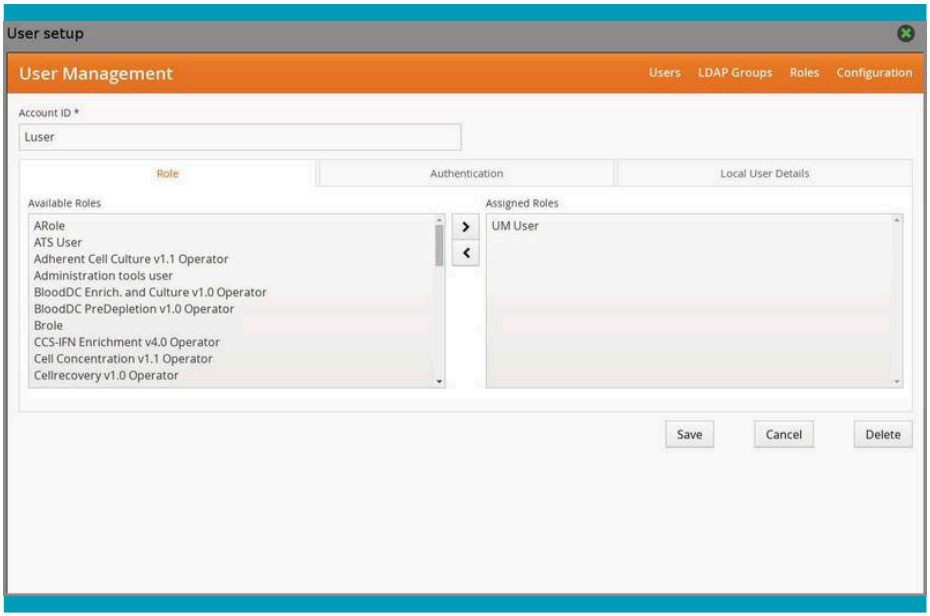


Bildschirm 10.16: Speichern erfolgreich

Das inaktive Konto wird nicht in der Benutzerliste angezeigt. Das Konto ist jedoch nach wie vor im Gerät gespeichert. Um dieses Konto anzuzeigen oder zu reaktivieren, **<Show Inactive>** mit einem Häkchen markieren (siehe Bildschirm 10.16) und das Verfahren in Abschnitt 10.2.7 ´Ändern der zugewiesenen Rollen eines Benutzers oder einer LDAP-Gruppe´.

10.2.9 Löschen von LDAP-Benutzern

1. Einen LDAP-Benutzer oder eine LDAP-Gruppe aus der Benutzerliste wählen.
2. Auf der Benutzerkonfigurationsseite auf **<Delete>** (Löschen) drücken (siehe Bildschirm 10.17).



Bildschirm 10.17: Löschen eines LDAP-Benutzers

3. Auf <Save> unten auf der Seite drücken, um zur Benutzerliste zurückzukehren.

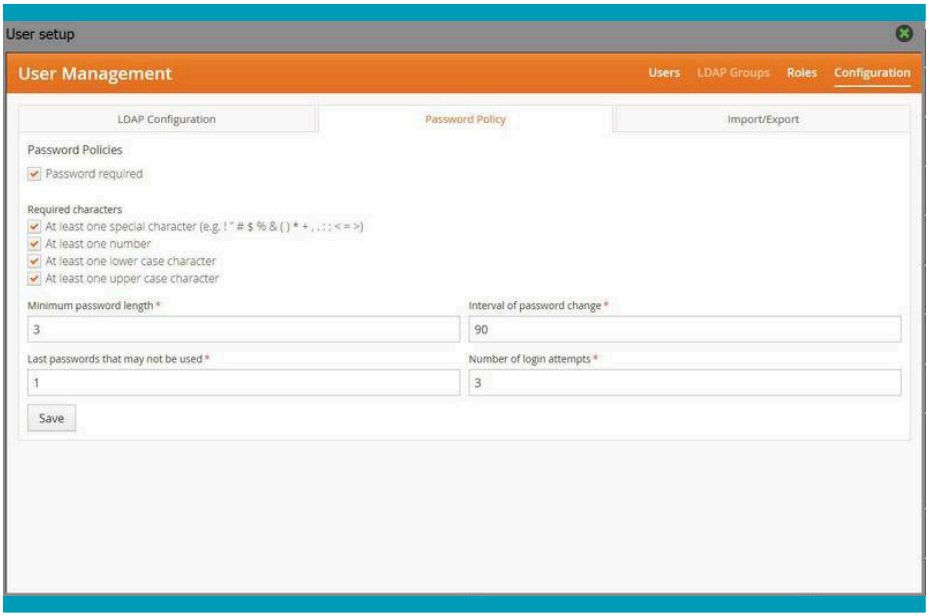
10.3 Konfigurieren der Passwortrichtlinien

Um die Passwortrichtlinien zu konfigurieren, auf <Configuration> in der rechten oberen Ecke drücken und die Registerkarte <Password Policy> (Passwortrichtlinien) wählen. Folgendes kann konfiguriert werden:

- Erforderliche Zeichen
- Länge des Passworts
- Ablaufdatum des Passworts (in Tagen)
- Letzte Passwörter, die nicht verwendet werden dürfen
- Maximale Anzahl von Anmeldeversuchen

Anmerkung: Das Ändern der Passwortrichtlinien betrifft nur die Benutzer, die danach angelegt werden. Die bereits bestehenden Benutzer sind nicht davon betroffen.

Anmerkung: Für das LDAP-Konto haben die LDAP-Passwortrichtlinien Vorrang vor den normalen Passwortrichtlinien.



Bildschirm 10.18: Konfigurieren der Passwortrichtlinien

10.4 Import und Export von Einstellungen für das User Management

Die Einstellungen für das UMS können von einem Gerät auf ein anderes übertragen werden. Der Prozess umfasst zwei Phasen:

(1) Kopieren zwischen USB-Stick und UMS Exchange Folder mit dem UMS Exchange Tool (UMS-Austausch)

(2) Import/Export in UMS in der Konfiguration der Benutzerverwaltung.

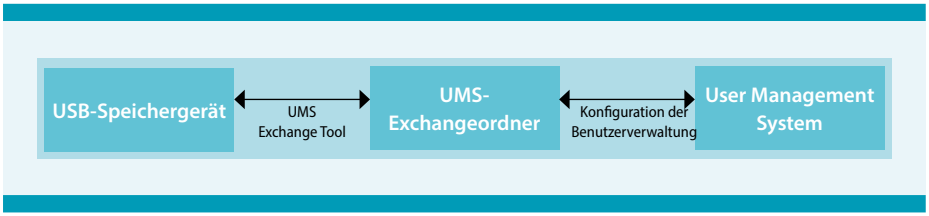


Abbildung 10.2: User Management System (Benutzerverwaltungssystem)

Das Musterverfahren gilt für die beiden folgenden Dateien:

- Importieren von SSL-(Secure Sockets Layer-)Zertifikatsdateien zur Einrichtung einer sicheren LDAP-Verbindung.
- Importieren und Exportieren von UMS-Einstellungsdateien zur Datensicherung oder Wiederverwendung in anderen UMS-Instanzen.

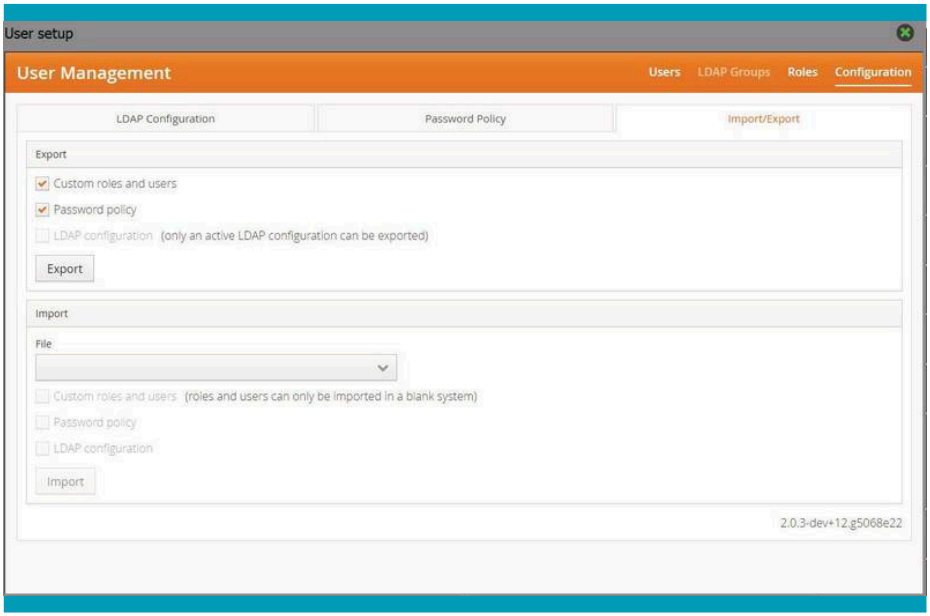
Anmerkung: Nur UMS-Benutzer mit der Administratorrolle 'Administration tools user' können auf diese Anwendung zugreifen.

10.4.1 Exportieren der Einstellungen der Benutzerverwaltung

WICHTIG

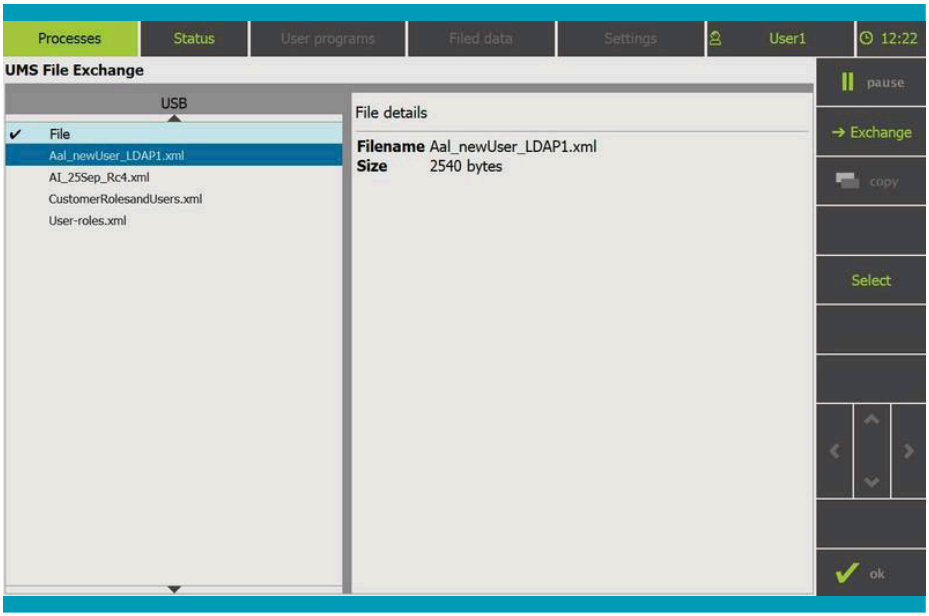
Rollen und Benutzer können nur in ein leeres System importiert werden..

1. Einen USB-Stick einstecken.
2. Zu <User Management> ▸ <Configuration> ▸ <Import/Export> gehen. Auf <Export> (Exportieren) drücken. Die UMS-Einstellungen werden in den UMS Exchange Folder auf dem Gerät exportiert.



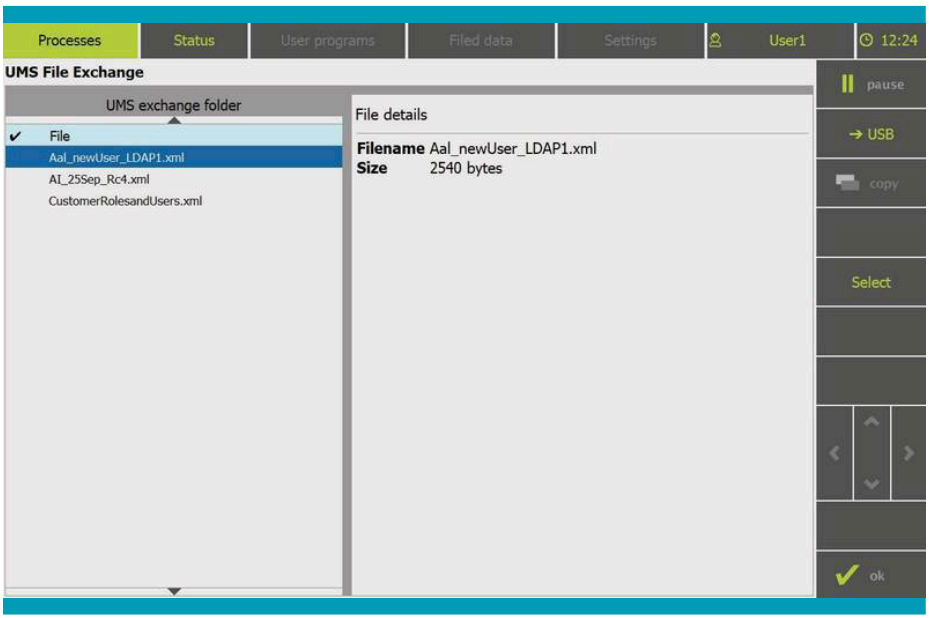
Bildschirm 10.19: Untermenü „Configuration" mit aktivem „Import/Export"

3. Um den <UMS File Exchange> (UMS-Dateiaustausch) durchzuführen, zu <Settings> ▸ <Tools>, < UMS File Exchange> gehen und auf <run> drücken.
4. Wenn USB in der linken Spalte erscheint, auf <Exchange> drücken, um den Inhalt des UMS Exchange Folders aufzulisten (siehe Bildschirm 10.20). Die Dateien im UMS-Exchangeordner werden in der linken Spalte angezeigt (siehe Bildschirm 10.21).



Bildschirm 10.20: Ausgewählte Datei und Menüschaltfläche „Exchange“

5. Die in das UMS zu übertragenden Dateien auswählen und auf <Select> (Auswählen) drücken.
6. Sobald alle zu übertragenden Dateien ausgewählt sind, auf <copy> (Kopieren) drücken, um die Übertragung zu starten.



Bildschirm 10.21: UMS-Exchangeordner mit ausgewählten Dateien

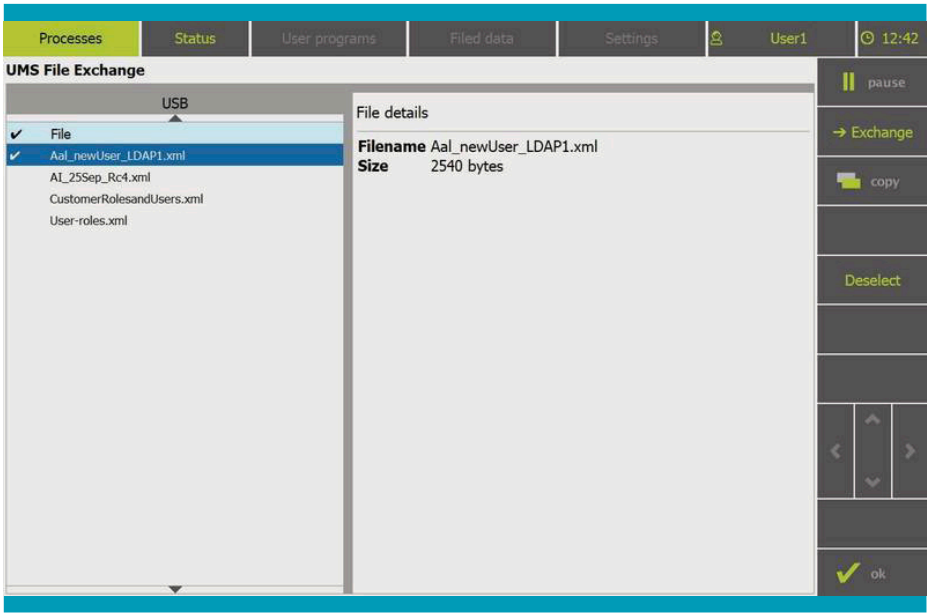
10.4.2 Importieren von UMS-Einstellungen

1. Einen USB-Stick einstecken.
   Sicherstellen, dass die Dateien im Stammordner des USB-Sticks sind (Dateien in Unterordnern werden nicht erkannt).

2. Zu <Processes> ▸ <Tools>, <UMS File Exchange> gehen und auf <run> drücken, um das Tool <UMS File Exchange> zu starten. Eine Dateiliste wird auf der linken Seite angezeigt.

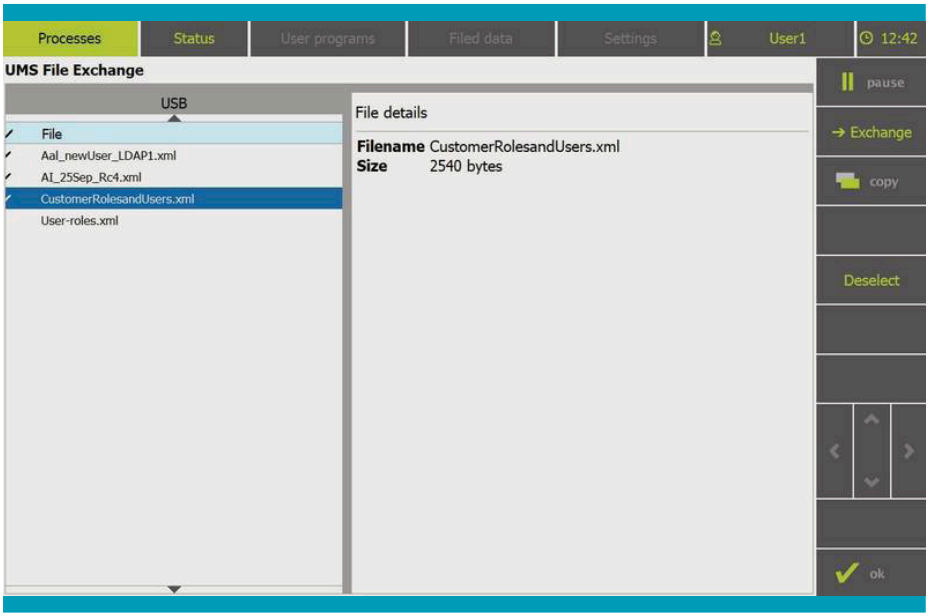
3. Wenn der UMS Exchange Folder angezeigt wird, auf <USB> in der Werkzeugleiste drücken. Sicherstellen, dass <USB> über der Dateiliste in der linken Spalte steht.

4. Die zu übertragenden Dateien auswählen und <Select> (Auswählen) drücken. Um eine Datei zu deselektieren, eine ausgewählte Datei wählen und auf <Deselect> drücken.



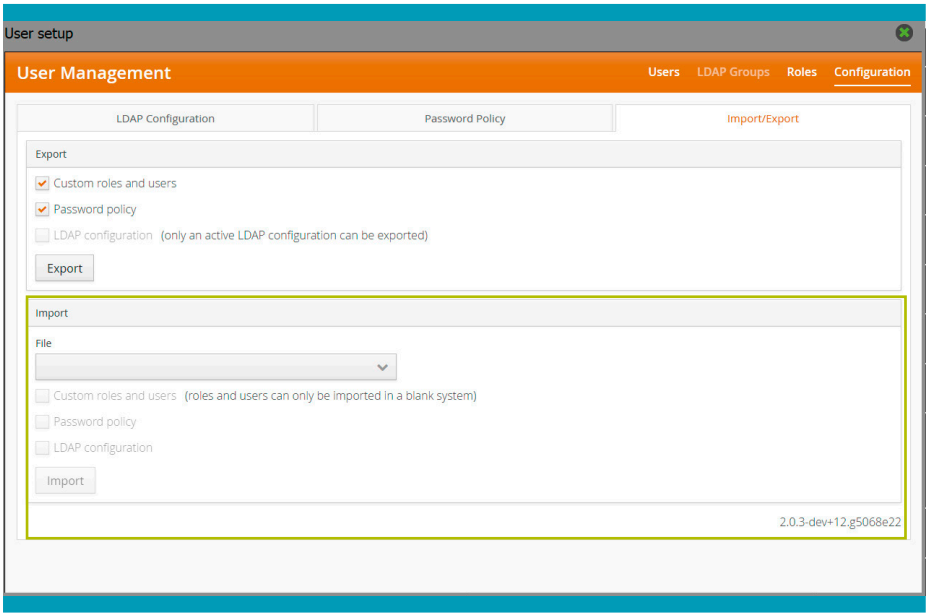
Bildschirm 10.22: Ausgewählte Datei und Menüschaltfläche „Select“

5. Sobald alle zu übertragenden Dateien ausgewählt sind, auf <copy> (Kopieren) drücken, um die Übertragung zu starten.



Bildschirm 10.23: USB-Ordner mit ausgewählten Dateien

6. Zu <User setup> ▸ <Configuration> ▸ <Import/Export> gehen. Die Datei unter <Import> wählen und auf <Import> drücken.



Bildschirm 10.24: Untermenü „Configuration“ mit aktiver Registerkarte „Import/Export“

11 Fehlerbehebung

In allen Fällen von Fehlfunktionen des Geräts oder Prozessstörungen wenden Sie sich an den Miltenyi Biotec Technical Support unter:

+49 2204 8306-3803
technicalsupport@miltenyi.com

Die lokalen Kontaktdaten des Miltenyi Biotec Technical Support finden Sie unter www.miltenyibiotec.com.

12 Rechtliche Hinweise

12.1 Beschränkte Garantie

Soweit nicht in einer gesonderten, mit diesem Miltenyi Produkt gelieferten Garantieerklärung oder einer schriftlich mit einem ordnungsgemäß befugten Vertreter von Miltenyi Biotec getroffenen Vereinbarung anderslautend festgelegt, unterliegt die von Miltenyi Biotec eingeräumte Garantie auf direkt von Miltenyi Biotec bezogene Produkte jenen Verkaufsbedingungen, zu denen der Kunde das Produkt von der jeweiligen Miltenyi Biotec Vertriebsorganisation erworben hat. Diese Verkaufsbedingungen sind auf Anfrage bzw. unter www.miltenyibiotec.com erhältlich. Je nach Land und Region können unterschiedliche Verkaufsbedingungen gelten. Nichts in diesem Dokument ist als zusätzlich eingeräumte Garantie zu verstehen.

Für Produkte, die von Drittanbietern oder Wiederverkäufern (z. B. einem örtlich zuständigen Miltenyi Biotec Vertreter) bezogen wurden, gelten unter Umständen andere Verkaufsbedingungen.

Weitere Angaben zu der auf das gekaufte Produkt geltenden Garantie sind dem Packzettel, der Rechnung, der Empfangsbestätigung oder sonstigen Verkaufsunterlagen zu entnehmen. Für einige Komponenten einer Produktkombination, die Sie erworben haben, gilt möglicherweise ein kürzerer Garantiezeitraum als auf dem Lieferschein, der Rechnung, Empfangsbestätigung oder anderen Verkaufsunterlagen angegeben (z. B. für Waren, die einer Haltbarkeitsdauer oder Veralterung unterliegen).

Die von Miltenyi Biotec auf dieses Produkt eingeräumte Garantie gilt nur für Mängel am Produkt, die auf Material- oder Verarbeitungsfehler zurückgehen und im ordnungsgemäßen Gebrauch auftraten. Sie gilt nicht für Produktmängel, die auf andere Ursachen zurückgehen, einschließlich, aber nicht beschränkt auf Mängel infolge Nutzung des Produkts in einer anderen als in diesem Handbuch ausdrücklich beschriebenen Weise, wie u. a. unsachgemäßer oder fehlerhafter Gebrauch; fehlerhafter Zusammenbau oder fehlerhafte Installation durch einen

Anwender oder einen Dritten; reguläre Abnutzung und Verschleiß; fahrlässiger oder fehlerhafter Betrieb, Handhabung, Lagerung, Wartung oder Reparatur; Missachtung der Bedienungsanleitungen; unzulässige Änderungen oder Umbauten von oder an Teilen dieses Produkts sowie Verwendung ungeeigneter Verbrauchsmaterialien, Zubehörteile oder Arbeitsmittel.

Die von Miltenyi Biotec eingeräumte Garantie gilt nicht für Verbrauchsmaterialien sowie Produkte, die WIE GESEHEN oder MIT ALLEN MÄNGELN erworben wurden. Nichts in diesem Dokument ist als zusätzlich eingeräumte Garantie zu verstehen.

Miltenyi Biotec muss unverzüglich informiert werden, wenn ein Anspruch unter einer solchen Garantie erhoben wird. Miltenyi Biotec wird bei Auftreten eines Material- oder Verarbeitungsfehlers während der Garantielaufzeit alle notwendigen Maßnahmen ergreifen, um das Gerät wieder in voll funktionsfähigen Zustand zu versetzen.

Haftungsbeschränkung:
Miltenyi Biotec haftet nicht für Schäden, die sich als direkte oder indirekte Folge der Nichteinhaltung einer ausdrücklichen oder implizierten Gewährleistung oder Bedingung für dieses Produkt ergeben.

In manchen Ländern, Staaten und Gerichtsbarkeiten ist der Ausschluss oder die Einschränkung der Haftung für Neben- oder Folgeschäden nicht zulässig, so dass die oben genannte Einschränkung bzw. der Ausschluss unter Umständen nicht auf Sie zutrifft. Diese Garantieerklärung räumt Ihnen bestimmte Rechte ein, zu denen je nach Land oder Gerichtsbarkeit weitere Rechte hinzutreten können.

12.2 Marken

CliniMACS, CentriCult und das Miltenyi Biotec-Logo sind eingetragene Marken oder Marken der Miltenyi Biotec und/oder ihrer verbundenen Unternehmen in verschiedenen Ländern weltweit.

ANHANG

Jeder Prozess, jedes Tool und jede Einstellung ist mit bestimmten Rechten verbunden, z. B. dem Recht 'Show' (Anzeigen) und dem Recht 'Start' (Starten). Mit dem Recht 'Show' ist das Tool, der Prozess bzw. die Einstellung auf der Registerkarte Process/Settings (Prozess/Einstellungen) sichtbar. Um den Prozess, das Tool bzw. die Einstellung zu verwenden, muss der betreffenden Benutzerrolle das Recht 'Start' zugewiesen sein. Komplexere Komponenten wie Audit Trail und User Management (Benutzerverwaltung) haben umfangreichere Rechte.

Prozess/Tool/Einstellungen/Komponente	Details
Process xxx right (Rechte für Prozess xxx)	• Show process xxx (Prozess xxx anzeigen) • Start process xxx (Prozess xxx starten)
Tool xxx right (Rechte für Tool xxx) • Backup Filed Data (Datensicherung für Dateien) • Custom Files (benutzerdefinierte Dateien) • Instrument check (Geräteprüfung) • License (Lizenz) • N2 Settings (N2-Einstellungen) • Network Settings (Netzwerkeinstellungen) • Set Time (Uhrzeit einstellen) • Settings Exchange (Einstellungen für Austausch) • SetVolume (Volumen einstellen) • Abschalten • UMSFileExchange exchange (Datenaustausch UMS-Dateien) • UMSSettings settings Process xxx right (UMS-Einstellungen für Rechte zum Prozess xxx)	• Show tool xxx (Tool xxx anzeigen) • Start tool xxx (Tool xxx starten)

Prozess/Tool/Einstellungen/Komponente	Details
Setting xxx right (Rechte für Einstellung xxx) • Info • Systemeinstellungen	• Show setting xxx (Einstellung xxx anzeigen) • Start setting xxx (Einstellung xxx starten)
Gerät	• Log file access via FTP (Zugriff auf die Protokolldatei über FTP) • Show injected programs (Injizierte Programme anzeigen) • Start injected programs (Injizierte Programme starten)
User Management (Benutzerverwaltung)	• Assign role (Rolle zuweisen) • Configure LDAP connection (LDAP-Verbindung konfigurieren) • Create role (Rolle anlegen) • Create user (Benutzer anlegen) • Export (Exportieren) • Import (Importieren) • Read Password Policy (Passwortrichtlinie einsehen) • Read details of foreign account (Details zum fremden Konto einsehen) • Read details of own account (Details zum eigenen Konto einsehen) • Read own user details (Eigene Benutzerdaten einsehen) • Read rights of foreign account (Rechte zum fremden Konto einsehen) • Read rights of own account (Rechte zum eigenen Konto einsehen) • Read role (Rolle einsehen) • Read user details (Benutzerdaten einsehen) • Set user active (Benutzer aktiv setzen) • Set user inactive (Benutzer inaktiv setzen) • Unlock user (Benutzer entsperren) • Update Password Policy (Passwortrichtlinien aktualisieren) • Update own user details (Eigene Benutzerdaten aktualisieren) • Update role (Rolle aktualisieren) • Update user details (Benutzerdaten aktualisieren)
Audit Trail Management (Audit Trail Verwaltung)	• Export audit trail events (Audit Trail Ereignisse exportieren) • Read audit trail events (Audit Trail Ereignisse einsehen) • Reset audit trail events (Audit Trail Ereignisse zurücksetzen)

Table A.1: Übersicht über die in der Software definierten Rechte

Standardrollen

Rollen	Tools/Rechte
ATS User (ATS-Benutzer)	Benutzer der Komponente Audit Trail • Audit Trail Management (Audit Trail Verwaltung)
Administration tools user (Benutzer von Verwaltungstools)	• Customer settings (Kundeneinstellungen) • Network settings (Netzwerkeinstellungen) • Platform configuration settings (Einstellungen für die Plattformkonfiguration) • Settings exchange (Einstellungen für Austausch) • System settings (Systemeinstellungen) • UMSFileExchange exchange (Datenaustausch UMS-Dateien)
File management user (Benutzer der Dateiverwaltung)	Ein Benutzer, der Tools zur Dateiverwaltung verwendet • Backup Filed Data (Datensicherung für Dateien) • Custom Files (benutzerdefinierte Dateien) • Log file access via FTP (Zugriff auf die Protokolldatei über FTP)
File system access (Zugriff auf Dateisystem)	Zugriff auf beliebige ausführbare Dateien im Dateisystem – kein Zugriff auf Rechte
Support tools user (Benutzer von unterstützenden Tools)	Ein Benutzer, der Tools verwenden kann, die die Ausführung von Anwendungen unterstützen • Chamber In (Kammer rein) • Chamber out (Kammer raus) • FormU Sensor (FormU-Sensor) • FormU Valves (FormU-Ventile) • FRAMrd • Gasmix Settings (Einstellungen für die Gasmischung) • Instrument check (Geräteprüfung) • Module Settings (Einstellungen für die Module) • Sealer (Schlauchschweißgerät)
UM Administrator (BM Administrator)	Administrator der Benutzerverwaltungskomponente User Management – alle Rechte
UM Service (BM Service)	Service User (Benutzer des Service) • User Management – all rights (Benutzerverwaltung – alle Rechte)
UM User (BM Benutzer)	Customer User (Spezifischer Benutzer) • User Management: Read details for own account (Details zum eigenen Konto einsehen) • User Management: Read rights for own account (Rechte für das eigene Konto einsehen)

Table A.2: Standardrollen

Miltenyi Biotec

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

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

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

Benelux
Miltenyi Biotec B.V.
Dellaertweg 9C
2316 WZ Leiden
Niederlande
macsnl@miltenyi.com
Kundenservice für:
Niederlande
0800 4020120
0800 4020100
Belgien
0800 94016
0800 99626
Luxemburg
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

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

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

Indien
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
Indien
+91 040 45175910
macsin@miltenyi.com

Italien
Miltenyi Biotec S.r.l.
Via Paolo Nanni Costa, 30
40133 Bologna
Italien
+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

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

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

Skandinavien und Baltikum
Miltenyi Biotec Norden AB
Medicon Village
Scheeletorget 1
223 81 Lund
Schweden
macsse@miltenyi.com
Kundenservice für:
Schweden
0200 111 800
+46 280 72 99

Dänemark
80 20 30 10
+46 46 280 72 99
Norwegen, Finnland, Island und Baltikum
+46 46 280 72 80
+46 46 280 72 99

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

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

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

www.miltenyibiotec.com

210-005-262/01 | Stand: 2026-03

Miltenyi Biotec vertreibt seine Produkte und Dienstleistungen weltweit. Den Kontakt für Ihr Land finden Sie unter **www.miltenyibiotec.com/local**.

CliniMACS, CentriCult und das Miltenyi Biotec-Logo sind eingetragene Warenzeichen oder Warenzeichen der Miltenyi Biotec B.V. & Co. KG und/oder ihrer verbundenen Unternehmen in verschiedenen Ländern weltweit. Copyright © 2026 Miltenyi Biotec und/oder verbundene Unternehmen. Alle Rechte vorbehalten.