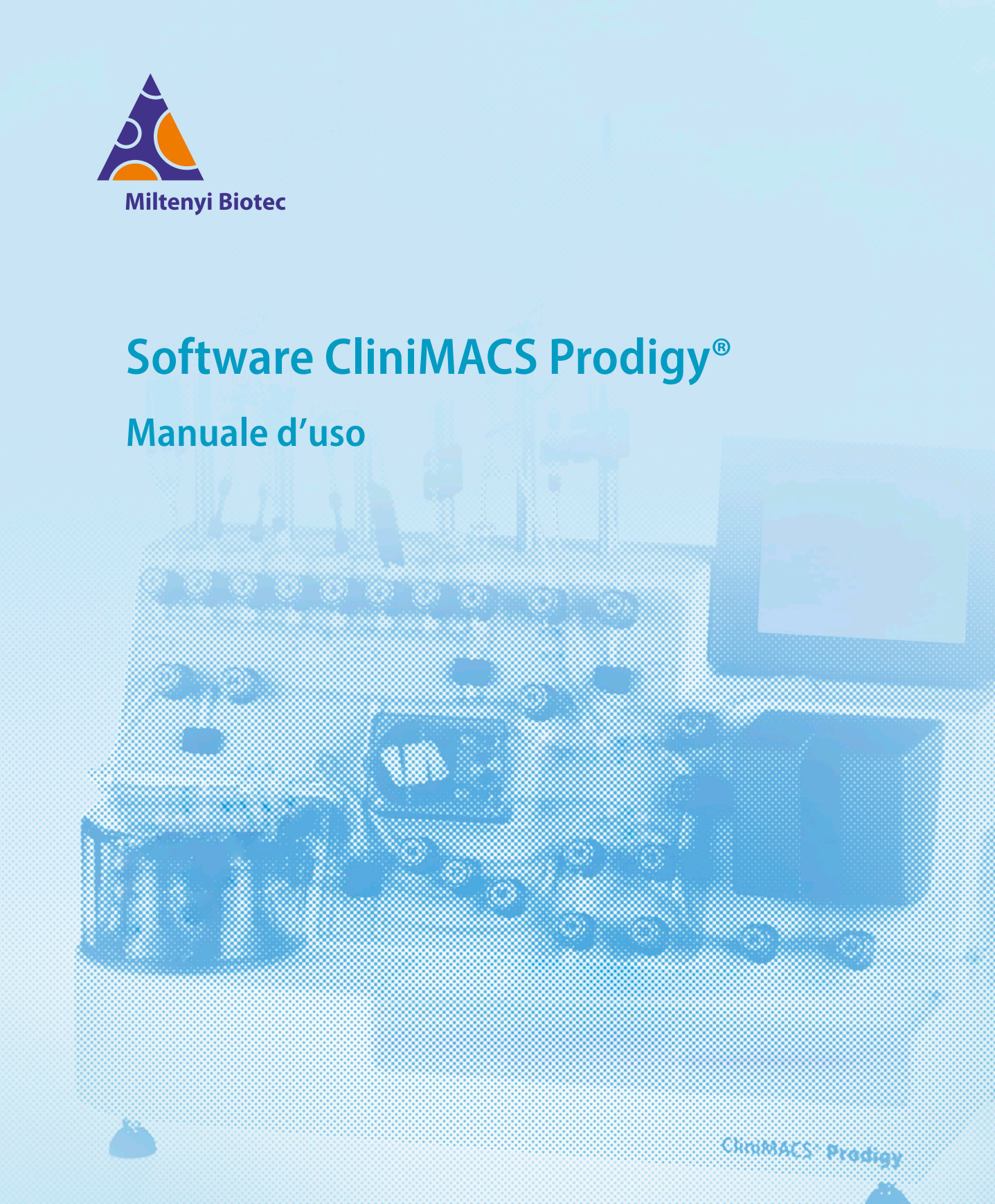
Miltenyi Biotec

Software CliniMACS Prodigy®

Manuale d’uso



I componenti del sistema CliniMACS, inclusi reagenti, set di tubi, strumenti e tampone PBS/EDTA, sono progettati, prodotti e testati secondo un sistema di qualità certificato ISO 13485. Nell'UE, i componenti del sistema CliniMACS sono disponibili come dispositivi medici con marcatura CE per il rispettivo uso previsto, salvo diversa indicazione. Negli Stati Uniti, il sistema CliniMACS CD34 Reagent, che include il CliniMACS Plus Instrument, il CliniMACS CD34 Reagent, il CliniMACS Tubing Set TS e il CliniMACS Tubing Set LS ed il CliniMACS PBS/EDTA Buffer, è stato approvato dalla FDA come dispositivo per uso umanitario (HUD), autorizzato dalla legge federale degli Stati Uniti per l'uso nel trattamento dei pazienti con leucemia mieloide acuta (LMA) in prima remissione completa. L'efficacia del dispositivo per questa indicazione non è stata dimostrata. Tutti gli altri prodotti della linea di prodotti CliniMACS sono disponibili per l'uso solo in caso di applicazione approvata come nuovo farmaco sperimentale (IND), di speciale autorizzazione per dispositivo sperimentale (IDE) o di un'approvazione della FDA.. In Australia, i seguenti componenti del sistema CliniMACS Prodigy sono inclusi nel Registro australiano dei beni terapeutici (ARTG) e sono quindi approvati per la fornitura: CliniMACS Prodigy, CliniMACS CD34 Reagent, i set di tubi CliniMACS Prodigy e CliniMACS PBS/EDTA Buffer. Solo i prodotti che sono inclusi nell'ARTG possono essere utilizzati in Australia. Le CliniMACS MicroBeads sono usate solo a scopo di ricerca e non per uso terapeutico o diagnostico umano.

Salvo diversamente specificato, i prodotti e i servizi di Miltenyi Biotec sono destinati esclusivamente per l'uso a scopo di ricerca, e non per scopo terapeutico o diagnostico.

Copyright © 2026 Miltenyi Biotec e/o sue affiliate. Tutti i diritti riservati.

È vietato riprodurre, archiviare in un sistema di recupero, trasmettere, pubblicare o distribuire la presente pubblicazione in ogni sua parte, in qualsiasi forma o con qualsiasi mezzo, elettronicamente, meccanicamente, mediante fotocopie, microfilm, registrazioni o altro, senza il previo consenso scritto di Miltenyi Biotec; fatto salvo quanto precede, i proprietari del sistema CliniMACS Prodigy possono comunque effettuare copie unicamente per scopi di formazione del personale sull'uso e la manutenzione dell'unità all'interno della loro azienda od organizzazione.

CliniMACS, CentriCult e il logo Miltenyi Biotec sono marchi registrati o marchi depositati di Miltenyi Biotec B.V. & Co. KG e/o sue affiliate in vari paesi in tutto il mondo. Tutti gli altri marchi citati nel presente manuale d'uso o in qualsiasi documento di accompagnamento sono di proprietà dei rispettivi proprietari e vengono utilizzati solo a scopo identificativo.

Software CliniMACS Prodigy®

Manuale d’uso

Versione software 2.2

Edizione: 2026-03

210-005-268/01

MD CE 0123

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

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

www.miltenyibiotec.com

Informazioni essenziali

Questo manuale d'uso contiene istruzioni, avvertenze, precauzioni, note e altre informazioni importanti per l'uso del software CliniMACS Prodigy. Per informazioni dettagliate sullo strumento, come lo schermo tattile e la configurazione generale, consultare il manuale d'uso dello strumento del CliniMACS Prodigy.

⚠ AVVERTENZA

L'utilizzo del sistema CliniMACS Prodigy deve essere eseguito solo da personale addestrato. Prima di mettere in funzione il sistema, leggere attentamente e comprendere le informazioni sulla sicurezza, le avvertenze, le precauzioni e le istruzioni per il corretto funzionamento del CliniMACS Prodigy fornite nelle istruzioni per l'uso dei componenti del sistema CliniMACS Prodigy e in tutte le raccomandazioni relative alla sicurezza pubblicate da Miltenyi Biotec. Queste istruzioni per l'uso includono, a titolo esemplificativo, le informazioni sulla sicurezza contenute nel manuale d'uso dello strumento del CliniMACS Prodigy, capitolo 'Informazioni importanti sulla sicurezza'. Prestare particolare attenzione a tutte le avvertenze visualizzate sullo strumento o fornite con i materiali di consumo e gli accessori, nonché alle note e alle informazioni importanti descritte nel presente manuale d'uso. Osservare sempre tutte le istruzioni e procedure durante l'utilizzo dello strumento, assicurandosi di rispettare tutte le informazioni sulla sicurezza, le avvertenze, le precauzioni e le istruzioni. La mancata osservanza delle informazioni importanti e di sicurezza, delle avvertenze, delle precauzioni, delle note aggiuntive e delle istruzioni contenute nelle istruzioni per l'uso potrebbe causare il malfunzionamento dello strumento, danni materiali, lesioni personali e/o morte. L'uso di apparecchiature in maniera difforme dalle istruzioni del fabbricante potrebbe compromettere la sicurezza dell'apparecchiatura. Conservare le istruzioni per l'uso per futuro riferimento. Devono essere accessibili e prontamente disponibili per tutto il personale responsabile dell'installazione, dell'utilizzo e della manutenzione, unitamente a tutta la documentazione riguardante la sicurezza e l'utilizzo dello strumento per il suo intero ciclo di vita.

Indice

1	**Introduzione**	**9**
1.1	Informazioni generali	9
1.2	Informazioni regolatorie	10
1.3	Leggi sulla protezione dei dati	10
1.4	A proposito di questo manuale	10
1.5	Documenti correlati	11
2	**Glossario**	**13**
2.1	Livello di pericolo	13
2.2	Convenzioni di stile e formattazione	14
2.3	Glossario dei simboli e dei termini	14
2.3.1	Termini specifici del software	15
3	**Informazioni importanti sulla sicurezza**	**17**
3.1	Istruzioni di sicurezza per il CliniMACS Prodigy	17
3.2	Istruzioni di sicurezza per il software	18
4	**Cibersicurezza**	**19**
4.1	Concetto di "difesa in profondità" per la sicurezza	19
4.1.1	Livello di protezione fisica	21
4.1.2	Livello dell'ambiente di rete	22
4.1.3	Livello del software dello strumento	24
4.1.4	Livello dell'utente	26
4.1.5	Livello di audit	26
4.1.6	Livello di gestione degli aggiornamenti	26
4.1.7	Livello di gestione delle vulnerabilità	27
4.1.8	Livello di backup e ripristino	27
4.1.9	Riepilogo della configurazione di sicurezza	28

5	**Software**	**29**
5.1	Concetto di base	29
5.2	Interfaccia grafica utente	31
5.2.1	Barra del menu e area dei contenuti	32
5.2.2	Barra di stato	32
5.2.3	Barra degli strumenti	33
5.2.4	Campi di inserimento	34
5.2.5	Finestre pop-up	35
6	**Operazioni di base**	**37**
6.1	Accendere lo strumento	37
6.2	Login	38
6.3	Logout	39
6.4	Shutdown (Spegnimento	39
6.5	Emergency Stop	39
6.6	Selezionare un processo applicativo	40
6.7	Eseguire un processo applicativo	41
6.8	Sospendere un processo applicativo	42
6.9	Stato dello strumento e del processo applicativo	43
6.10	Acquisizione di immagini	44
6.10.1	Camera di rilevazione strati	45
6.10.2	Camera con microscopio	46
7	**Accesso ai dati**	**47**
7.1	Recupero dei log delle applicazioni	47
7.1.1	Visualizzazione ed esportazione dei logfile su USB	47
7.1.2	Recupero tramite FTP	49
7.1.3	Recuperare i file tramite la condivisione di file	50
7.2	Recupero di audit trail	51
7.2.1	Visualizzazione di audit trail	52
7.2.2	Esportazione di audit trail	53
7.2.3	Eliminazione di audit trail	55

8	**Strumenti e impostazioni utente**	**57**
8.1	Accesso agli strumenti e alle impostazioni utente	57
8.2	Tools (Strumenti)	58
8.2.1	Info tool (Strumento Info)	58
8.2.2	Backup Filed Data	59
8.2.3	Chamber In	63
8.2.4	Chamber Out	63
8.2.5	Shutdown (Spegnimento)	63
8.2.6	Recovery (Recupero)	64
8.2.7	Strumento Gas Mix (miscela dei gas)	64
8.2.8	Instrument Check (Controllo strumento)	64
8.2.9	Column Load (Caricamento colonna)	64
8.2.10	Custom Files (File personalizzati)	65
8.2.11	Sealer (Saldatore)	65
8.3	User settings (impostazioni utente)	65
8.3.1	Set time (Imposta ora)	65
8.3.2	Network Settings (Impostazioni di rete)	65
8.3.3	Custom settings (Impostazioni personalizzate)	65
8.3.4	Module settings (Impostazioni modulo)	66
8.3.5	Settings exchange tool (Strumento di scambio impostazioni)	67
8.3.6	Set Volume (Imposta volume)	71
8.3.7	N_2 Settings (Impostazioni N_2)	71
9	**Integrazione di rete**	**73**
9.1	Connessione a una rete locale	74
9.2	Connessione a un server LDAP	76
9.3	Connessione a un drive di rete	79
9.4	Configurazione del trasferimento di file tramite FTP	82
9.4.1	Configurazione dello strumento	83
9.4.2	Connessione con client FTP	84
9.5	Connessione a un server di posta elettronica	85
9.6	Abilitazione della sincronizzazione dell'ora di rete	91

10 Gestione degli utenti 93

10.1 Informazioni generali 93
10.2 Gestione di ruoli e account 96
10.2.1 Accesso a User Management 96
10.2.2 Creazione di un nuovo ruolo 97
10.2.3 Modifica dei diritti assegnati ai ruoli 98
10.2.4 Aggiunta di un utente locale 99
10.2.5 Aggiunta di utenti LDAP 102
10.2.6 Aggiunta di gruppi LDAP 104
10.2.7 Modifica dei ruoli assegnati a un utente o a un gruppo LDAP 105
10.2.8 Disattivazione utenti locali 106
10.2.9 Eliminazione utenti LDAP 108
10.3 Configurarazione dei criteri password 109
10.4 Impostazioni di Import ed Export in User Management 110
10.4.1 Impostazioni di Export in User Management 110
10.4.2 Importazione impostazioni in UMS 113

11 Risoluzione dei problemi 115

12 Note legali 117

12.1 Garanzia limitata 117
12.2 Marchi commerciali 118

APPENDICE

1 Introduzione

1.1 Informazioni generali

Il software sul CliniMACS Prodigy include il software di base e vari software applicativi.

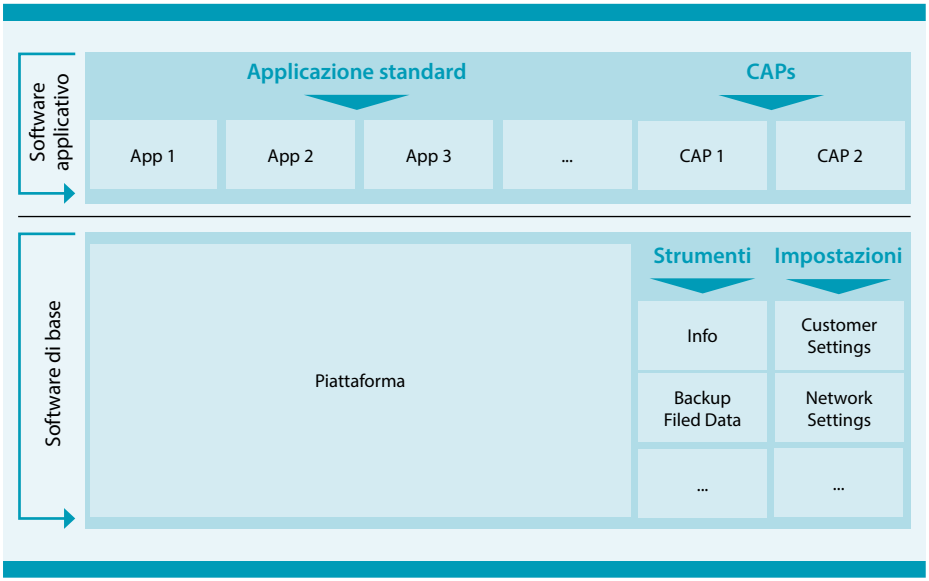


Figura 1.1: Panoramica del software dello strumento

Il software di base controlla lo strumento e l'esecuzione delle procedure di applicazione e fornisce i servizi essenziali descritti nei diversi capitoli e sezioni.

Il software di base è indicato come "software" all'interno di questo manuale d'uso.

Il software di applicazione viene eseguito dal software di base e fornisce le procedure di applicazione e le interfacce utente per il funzionamento del

CliniMACS Prodigy a seconda dell'uso previsto:

- come parte del sistema CliniMACS Prodigy per la separazione cellulare
- come parte del sistema CliniMACS Prodigy per la produzione di terapie geniche e a base cellulare è concepito per l'esecuzione di specifiche attività di manipolazione genetica e/o manipolazione estensiva (come proliferazione, differenziazione) di cellule umane

Il software di base e ciascuna applicazione sono entità indipendenti, il che consente l'aggiornamento separato di una nuova applicazione senza modificare il software di base.

1.2 Informazioni regolatorie

Il software è sviluppato in conformità alla norma IEC/EN 62304. Inoltre, il software di base del CliniMACS Prodigy è stato sviluppato per supportare la conformità a GAMP 5, EudraLex Volume 4 Allegato 11 (EU GMP Allegato 11) e 21 CFR Parte 11.

I requisiti di cibersicurezza sono soddisfatti in base allo standard IEC 81001-5-1, compresi i test di penetrazione eseguiti da una società terza.

La panoramica completa delle informazioni normative, compreso l'uso previsto, è parte del manuale d'uso dello strumento del CliniMACS Prodigy.

1.3 Leggi sulla protezione dei dati

Quando si elaborano dati personali con il sistema CliniMACS Prodigy, si consiglia vivamente all'utente di agire con discrezione. L'utente/utilizzatore è responsabile della conformità alle leggi e ai regolamenti vigenti in materia di protezione dei dati.

Nel rispetto dei principi della privacy by design e by default, Miltenyi ha implementato misure di sicurezza, in particolare il concetto di difesa in profondità (vedere sezione 4.1 ´Concetto di "difesa in profondità" per la sicurezza´).

1.4 A proposito di questo manuale

Questo manuale d'uso fornisce le informazioni necessarie per la configurazione e il funzionamento sicuro del software di base. Solo il software di base versione 2.2 rientra nell'ambito di questo manuale d'uso.

1.5 Documenti correlati

Il manuale d'uso dello strumento del CliniMACS Prodigy descrive l'hardware e il sistema dello strumento CliniMACS Prodigy. Il manuale d'uso dello strumento è fornito insieme a questo manuale.

Il manuale d'uso dello strumento include:

- Avvertenze, precauzioni, note
- Informazioni regolatorie
- Dati tecnici
- Altre informazioni importanti

Se si utilizza il CliniMACS Prodigy insieme al MACS® TubeSealer, al CliniMACS Electroporator, alla CliniMACS Formulation Unit o al CliniMACS Workbench, consultare i relativi manuali d'uso:

- Manuale d'uso del MACS TubeSealer
- Manuale d'uso del CliniMACS Electroporator
- Manuale d'uso della CliniMACS Formulation Unit
- Manuale d'uso del CliniMACS Workbench

Una panoramica completa degli accessori, dei componenti e degli strumenti MACS GMP disponibili si trova nel manuale d'uso dello strumento del CliniMACS Prodigy.

Per informazioni su applicazioni specifiche, contattare Miltenyi Biotec Technical Support.

2
Glossario

2.1 Livello di pericolo

Il colore e la parola di segnalazione di un messaggio di avvertimento dipendono dal livello di pericolo. Il livello di pericolo classifica il pericolo come descritto di seguito. Il livello, il tipo e la fonte di pericolo, nonché le potenziali conseguenze, i divieti e le misure sono indicati come segue.

⚠ AVVERTENZA

Indica una situazione di pericolo che, se non evitata, potrebbe causare morte o gravi lesioni.

⚠ ATTENZIONE

Indica una situazione di pericolo che, se non evitata, potrebbe causare lesioni lievi o moderate.

AVVISO

Indica informazioni considerate importanti, ma non riguardanti pericoli (ad es. messaggi relativi a danni materiali).

IMPORTANTE

Avvisa l'utilizzatore di importanti prassi o informazioni non correlate a lesioni personali né a danni materiali.

2.2 Convenzioni di stile e formattazione

Il testo in **<verde chiaro>** indica elementi dell'interfaccia grafica utente (ad esempio pulsanti, finestre di dialogo o voci di gestione utente).

2.3 Glossario dei simboli e dei termini

Una panoramica dei simboli e dei termini generali utilizzati per il sistema CliniMACS Prodigy è fornita nel manuale d'uso dello strumento del CliniMACS Prodigy. Il glossario dei simboli riporta i simboli usati per l'etichettatura dei prodotti CliniMACS.

2.3.1 Termini specifici del software

Processo applicativo	Software per il processamento cellulare, sviluppato da Miltenyi Biotec
ATS Audit Trail System	Componente software che tiene traccia e registra gli eventi, le azioni, gli input dell'utente e le modifiche apportate all'interno del software CliniMACS Prodigy
CAP	Processo applicativo personalizzato (Customized Application Process)
FTP File Transfer Protocol	Protocollo di comunicazione standard utilizzato per il trasferimento di file da un server a un client su una rete informatica
LDAP Lightweight Directory Access Protocol	Protocollo applicativo per l'accesso e la gestione di servizi di directory distribuiti su una rete di protocollo Internet
MD5	Algoritmo per la creazione di checksum utilizzato allo scopo di verificare l'integrità dei dati rispetto a un danneggiamento involontario
SMB Server Message Block	Protocollo di comunicazione utilizzato per condividere file, stampanti, porte seriali e dispositivi di comunicazione vari tra i nodi di una rete
SMTP Simple Mail Transfer Protocol	Protocollo di comunicazione per la trasmissione di messaggi di posta elettronica
Processo applicativo standard	Processo applicativo precedentemente validato fornito da Miltenyi Biotec
UMS User Management System	Componente software per gestire e controllare l'accesso degli utenti alle varie funzioni dello strumento

3

Informazioni importanti sulla sicurezza

3.1 Istruzioni di sicurezza per il CliniMACS Prodigy

Per informazioni dettagliate sulla sicurezza dello strumento, consultare il manuale d'uso dello strumento del CliniMACS Prodigy.

3.2 Istruzioni di sicurezza per il software

IMPORTANTE

Il controllo degli accessi allo strumento deve essere validato prima dell'uso. Proteggere il proprio nome utente e la password. Si consiglia di preparare una soluzione di emergenza (vedere capitolo 10 ´Gestione degli utenti´). In caso di accesso non riuscito durante l'esecuzione di un processo, contattare Miltenyi Biotec Technical Support.

- Prima di utilizzare lo strumento con la versione software 2.2, leggere il capitolo 3 ´Informazioni importanti sulla sicurezza´ nel manuale d'uso dello strumento del CliniMACS Prodigy e tutte le altre informazioni contenute nel presente manuale d'uso del software, comprese le istruzioni di sicurezza e d'uso.
- Prestare particolare attenzione a tutte le avvertenze visualizzate sullo strumento.
- Non leggere e seguire queste linee guida può portare a un uso improprio o non corretto e causare danni allo strumento. L'uso improprio potrebbe inoltre causare gravi lesioni personali, morte, risultati imprevedibili, malfunzionamento dello strumento e usura prematura dei componenti, riducendo la durata dello strumento. Tali azioni possono invalidare la garanzia.
- Conservare il manuale d'uso e tutte le altre istruzioni di sicurezza e operative fornite con lo strumento in un luogo sicuro e accessibile a tutti gli utenti per future consultazioni.
- Tutte le procedure di processamento devono essere eseguite solo da personale addestrato. L'utente/utilizzatore deve avere una conoscenza generale del processamento cellulare e conoscenze specifiche in materia di biosicurezza.
- Solo il fornitore di servizi autorizzato Miltenyi Biotec locale deve installare, mantenere o riparare lo strumento.
- La comunicazione e l'accesso ai dati tra il software e il server esterno o l'applicazione esterna devono essere validati prima dell'uso.
- In caso di timori seri circa l'uso sicuro dello strumento, contattare Miltenyi Biotec Technical Support.
- In caso di problemi o malfunzionamenti, contattare Miltenyi Biotec Technical Support.

4

Cibersicurezza

4.1 Concetto di "difesa in profondità" per la sicurezza

La cibersicurezza è una responsabilità condivisa tra Miltenyi Biotec e gli utenti. Il software è progettato con misure di sicurezza integrate per proteggere dalle minacce più comuni. Gli utilizzatori devono svolgere un ruolo attivo nella salvaguardia dei dati e nel mantenimento di pratiche sicure. In linea con l'uso previsto, si raccomanda un modello di difesa in profondità (defense-in depth) con i seguenti obiettivi:

- Prevenzione dell'impatto negativo sulla qualità del prodotto cellulare e del ritardo nella sua produzione
- Integrità dei protocolli, dei processi e dei dati di audit
- Integrità della configurazione del dispositivo
- Disponibilità dello strumento per il processamento cellulare
- Accesso consentito solo al personale addestrato e autorizzato

Il modello di difesa in profondità è strutturato nei seguenti livelli:

- Livello di protezione fisica
- Livello dell'ambiente di rete
- Livello del software dello strumento
- Livello dell'utente
- Livello di audit
- Livello di gestione degli aggiornamenti
- Livello di gestione delle vulnerabilità
- Livello di backup e ripristino

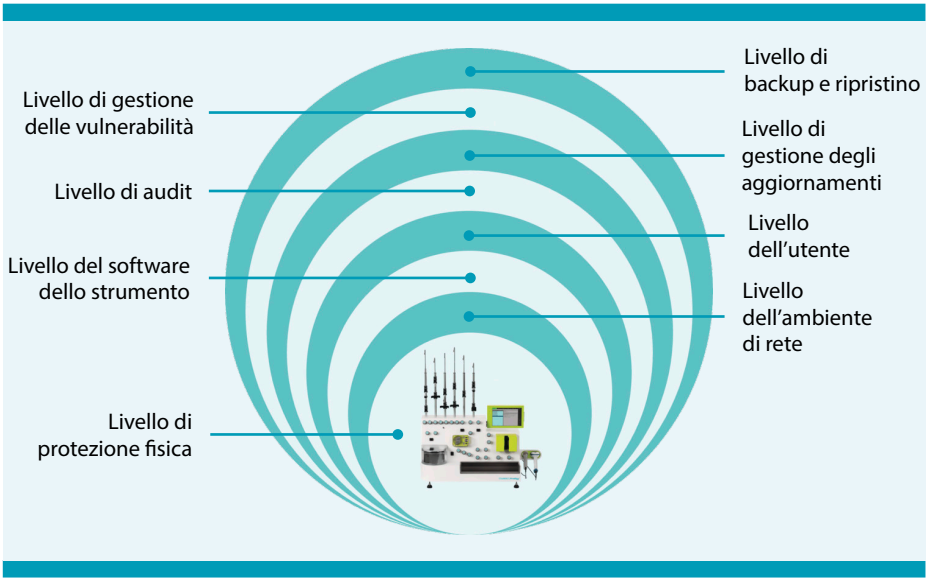


Figura 4.1: Livelli del concetto di difesa in profondità

4.1.1 Livello di protezione fisica

Lo strumento è dotato delle seguenti interfacce fisiche per la connessione dei diversi componenti, accessori e strumenti (vedere la Tabella 4.1). Il cliente ha la responsabilità di garantire che solo il personale autorizzato abbia accesso fisico al prodotto e deve prevedere processi adeguati per controllare e monitorare l'accesso fisico.

Interfaccia	Finalità
Porta USB	Connettere allo strumento le periferiche approvate, come la tastiera esterna o il lettore di codici a barre. Per connettere lo strumento alla rete è possibile usare un adattatore da USB a Ethernet. Le penne USB possono essere utilizzate per trasferire protocolli, immagini e logfile dallo strumento e programmi/aggiornamenti allo strumento, oltre che per l'installazione dello strumento.
Schermo tattile	Dispositivo per l'immissione dei dati utilizzato dal personale di manutenzione e assistenza e dagli operatori.
CAN bus/alimentazione Interfaccia CAN	L'interfaccia consente di connettere lo strumento a dispositivi aggiuntivi, come CliniMACS Electroporator o CliniMACS Formulation Unit.
Connettore per TubeSealer	Fornisce l'alimentazione a MACS TubeSealer, un saldatore termico installato su CliniMACS Prodigy. Non è un'interfaccia dati.
Connettore allarme	Connettore per circuito del relè per connettere lo strumento a un sistema di allarme esterno. Non è un'interfaccia dati.

Tabella 4.1: Interfacce e periferiche dello strumento

Le porte USB supportano la connessione delle penne USB. Anche se le connessioni USB sono controllate dal sistema operativo e da applicazioni, è responsabilità del cliente assicurarsi che con lo strumento vengano utilizzate solo penne USB approvate e controllate.

Nota: sono supportate solo penne USB in formato FAT32.

La manipolazione impropria (ad es. la forza fisica) di interfacce o accessori può danneggiare le interfacce fisiche dello strumento compromettendone il funzionamento, oltre a costituire un rischio residuo.

4.1.2 Livello dell'ambiente di rete

Lo strumento deve essere utilizzato in un segmento di rete protetto e separato da altri segmenti. Una possibile configurazione in cui lo strumento fa parte di una rete di strumenti isolata è mostrata nella Figura 4.2.Un router separa i diversi segmenti di rete e controlla il flusso di dati tra di loro.

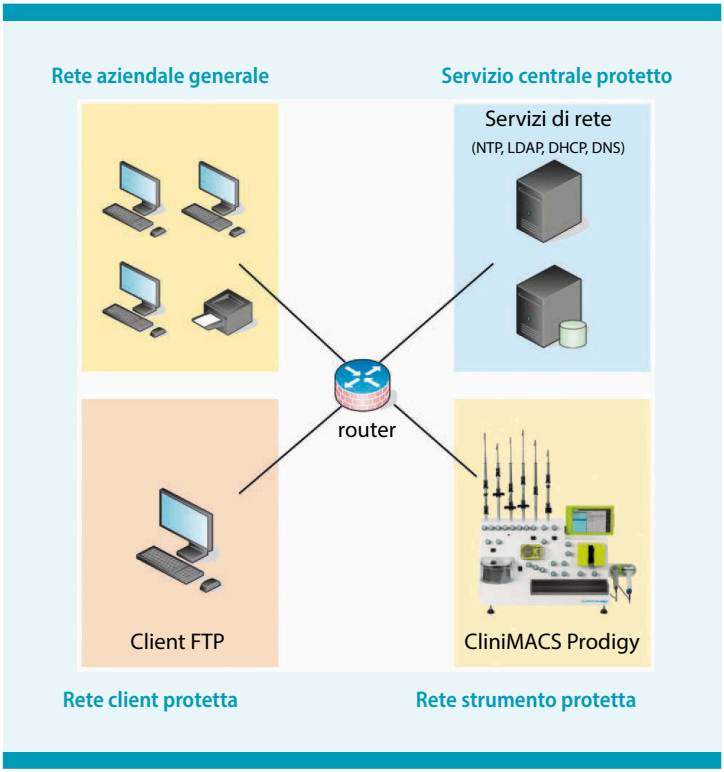


Figura 4.2: Diagramma della rete

Lo strumento fornisce principalmente funzionalità per la connessione ad altri sistemi della rete. I protocolli di rete supportati sono elencati nella Tabella 4.2.

Interfaccia	Finalità	Porta	Commento
FTP	Accesso al logfile in sola lettura tramite FTP	20 – 21	L'uso di FTP trasmette i logfile e le password in testo non crittografato attraverso la rete. Si raccomanda l'uso di un account utente dedicato per l'accesso ai dati tramite FTP allo scopo di limitare il rischio per il servizio FTP e impedire il 'lateral movement' nel caso in cui l'account utente venga compromesso. Di default il servizio FTP è disattivato.
NTP	Sincronizzazione oraria	123	–
DNS (client)	Risoluzione dei nomi host in indirizzi IP	53 (UDP)	–
Richiesta/risposta ICMP echo (server)	Controllo della connettività di rete allo strumento	N/A	–
DHCP (client)	Configurazione di rete automatica dello strumento	68 (UDP)	–
LDAP	Login allo strumento con le credenziali Active Directory gestite a livello centrale	389	Protocollo non sicuro, da utilizzare solo se LDAPS non è supportato
LDAPS	Versione protetta di LDAP	636	Una variante sicura di LDAP. Richiede una corretta configurazione, vedere sezione 9.2 'Connessione a un server LDAP'.
SMB	Condivisione di file	445	È supportata la condivisione autenticata. Richiede la configurazione, vedere sezione 9.3 'Connessione a un drive di rete'
SMTP	Notifica via mail	25, 2525, 465, 587	Autenticazione supportata. Richiede una corretta configurazione, vedere la sezione 9.5 'Connessione a un server di posta elettronica'
SMTPS	Versione protetta di SMTP	465, 587	Una variante sicura di SMTP. Richiede una corretta configurazione, vedere la sezione 9.5 ´Connessione a un server di posta elettronica´

Tabella 4.2: Connessioni e protocolli di rete

IMPORTANTE
Fatta eccezione per l'FTP, per tutti i servizi sono supportati protocolli sicuri. Si consiglia vivamente di attivare solo le funzioni di sicurezza elencate nella Tabella 4.2. Per questioni di compatibilità, sono supportate versioni non sicure dei protocolli. Se per motivi di compatibilità è necessario usare un protocollo non sicuro, il cliente deve adottare adeguate misure di mitigazione.

Il cliente ha la responsabilità di garantire che solo il personale autorizzato abbia accesso allo strumento e alle reti utilizzate per trasferire i protocolli attivati. Devono essere predisposti processi idonei per il controllo e il monitoraggio degli accessi alla rete. Inoltre, lo strumento non deve essere esposto direttamente a Internet.

4.1.3 Livello del software dello strumento

Lo strumento usa un sistema operativo Linux personalizzato. Per ridurre al minimo la superficie di attacco del software dello strumento, sono abilitati solo il software, servizi e funzionalità del kernel necessari.

L'accesso al BIOS dei PC dello strumento è consentito solo al personale di assistenza addestrato di Miltenyi. Il BIOS è configurato in modo da impedire l'avvio da supporti esterni e garantire l'integrità del software dello strumento.

Sono state adottate misure per garantire che solo il software autorizzato possa essere eseguito sullo strumento. Il nuovo software viene installato sullo strumento tramite una penna USB. L'avvio automatico del software dalla penna USB è precluso e l'operatore non può avviare le applicazioni direttamente dalla penna USB.

L'eventuale software aggiuntivo che deve essere generalmente disponibile sullo strumento va installato utilizzando un programma di installazione fornito con questo software. Per far sì che solo il software originale di Miltenyi Biotec necessario per lo strumento possa essere installato, sono stati previsti diversi controlli. In particolare, il programma di installazione controlla la data di scadenza del pacchetto di installazione e la firma elettronica del software da installare sullo strumento. Se uno dei controlli non viene superato, il software non può essere installato. Prima di eseguire l'installazione, è necessario aggiungere il pacchetto software, ovvero copiarlo nella memoria volatile dello strumento, utilizzando lo strumento Custom Files. Questo strumento serve a garantire che, oltre ai formati eseguibili proprietari, solo i file originali firmati da Miltenyi Biotec possano essere copiati nello strumento per essere eseguiti.

L'installazione di una nuova versione del software dello strumento è descritta di seguito nella sezione 4.1.6 ´Livello di gestione degli aggiornamenti´.

L'installazione delle nuove versioni del software dello strumento o del software applicativo personalizzato viene effettuata da Miltenyi Biotec Technical Support.

Nel sistema non è presente alcun software per il rilevamento di malware in quanto non adatto a questo prodotto. Il rischio di malware viene comunque controllato tramite il concetto di difesa in profondità.

Il software e gli strumenti applicativi validano gli input dell'utente per verificare la plausibilità. Tale validazione comprende, tra l'altro, la validazione dell'intervallo per gli input numerici, quella dei numeri di lotto e di prodotto dei materiali di consumo e i controlli di plausibilità per gli inserimenti.

Il software e le applicazioni non richiedono informazioni personali di natura sanitaria durante l'uso; permane un rischio basso che queste vengano inserite dall'operatore durante l'esecuzione dell'applicazione. È responsabilità dell'utente/utilizzatore assicurarsi che vengano rispettati i regolamenti vigenti in materia di privacy.

È possibile esportare protocolli e dati di log dallo strumento. I dati esportati sono accompagnati da hash di file per consentire all'operatore di verificare che l'esportazione e il trasferimento a un sistema a valle siano andati a buon fine e che i dati non siano stati danneggiati dal trasferimento. L'algoritmo usato al momento è MD5.

L'accesso al software per finalità di manutenzione e alle funzionalità limitate delle procedure applicative è possibile solo per Miltenyi Biotec Technical Support, e nelle normali operazioni non è disponibile per il cliente. L'accesso è possibile per gli utenti che effettuano il login con l'account dell'assistenza o con una penna USB dell'assistenza (ovvero una penna USB contenente le informazioni di autenticazione) e il PIN associato o attraverso la funzionalità di accesso remoto dello strumento Info insieme a un PIN monouso fornito da Miltenyi Biotec. Solo Miltenyi Biotec Technical Support ha accesso alle credenziali dell'account di assistenza e alla penna USB dell'assistenza. Il Supporto Tecnico può fornire un PIN monouso da utilizzare durante l'assistenza da remoto.

IMPORTANTE

Non sono state previste misure di protezione contro la lettura o la manipolazione intenzionale dei dati esportati. Il cliente è tenuto ad assicurarsi che solo il personale autorizzato abbia accesso ai dati esportati.

4.1.4 Livello dell'utente

Tutti gli accessi ai componenti possono essere protetti tramite le impostazioni configurabili della gestione utenti. Il cliente deve assicurarsi che vengano applicate le istruzioni e le raccomandazioni descritte in questo documento.

Deve inoltre assicurarsi che solo il personale addestrato e autorizzato abbia accesso allo strumento e che vengano osservate le migliori pratiche comuni relative all'utilizzo delle password nonché le normative vigenti.

4.1.5 Livello di audit

Il sistema di audit trail registra le informazioni sulle azioni eseguite sullo strumento, ad es. gli inserimenti dell'operatore durante l'esecuzione di un'applicazione o le modifiche alla configurazione dello strumento. Se l'audit trail è abilitato, le azioni vengono registrate nell'audit trail dello strumento. Il cliente deve assicurarsi che vengano osservate le istruzioni e le raccomandazioni descritte in questo documento.

Anche se i dati di audit trail sono generati dallo strumento, una gestione impropria di tali dati costituisce un rischio residuo. Al fine di mitigare questo rischio, la sicurezza e la gestione dei dati di audit trail (ad es. esportazione, archiviazione, cancellazione e revisione) da parte del cliente devono essere conformi ai regolamenti vigenti.

4.1.6 Livello di gestione degli aggiornamenti

Gli aggiornamenti di sicurezza vengono distribuiti mediante pacchetti di aggiornamento. Miltenyi Biotec informerà il cliente quando sarà disponibile un nuovo software.

Gli aggiornamenti del software dello strumento devono essere eseguiti esclusivamente da Miltenyi Biotec Technical Support. Gli aggiornamenti vengono consegnati e installati come descritto nelle procedure operative standard (POS) di Miltenyi Biotec. Gli aggiornamenti sono contenuti in pacchetti dedicati contenenti il nuovo software dello strumento e il software che esegue l'installazione effettiva. Vengono forniti in una penna USB. Per garantire l'integrità del pacchetto, tutti i componenti sono firmati crittograficamente. Ciò viene controllato prima di avviare l'installazione. Contattare Miltenyi Biotec Technical Support per richiedere un aggiornamento dello strumento.

4.1.7 Livello di gestione delle vulnerabilità

Per segnalare una vulnerabilità di sicurezza o un incidente riguardante il prodotto o uno dei suoi componenti, contattare Miltenyi Biotec Technical Support (vedere il capitolo 11 ´Risoluzione dei problemi´).

4.1.8 Livello di backup e ripristino

Lo strumento fornisce solo la funzionalità di backup per protocolli e dati. Il cliente deve assicurarsi che il backup di questi dati venga effettuato regolarmente e in conformità con i regolamenti vigenti. Nel caso in cui non si riesca a utilizzare il software dello strumento, contattare Miltenyi Biotec Technical Support.

4.1.9 Riepilogo della configurazione di sicurezza

Nelle sezioni precedenti sono state illustrate le misure di sicurezza in essere e quelle raccomandate da adottare per l'uso sicuro di CliniMACS Prodigy. Queste misure riguardano sia la configurazione dello strumento, sia procedure e norme che ne rafforzano la sicurezza. Si raccomandano le seguenti misure:

- Assicurarsi che solo il personale autorizzato abbia accesso fisico allo strumento e alle sue interfacce fisiche.
- Assicurarsi che l'accesso alla rete a cui lo strumento è connesso sia limitato al personale autorizzato e ai sistemi autorizzati.
- Abilitare l'autenticazione e l'autorizzazione su ogni strumento in modo che solo il personale autorizzato possa accedere al software dello strumento.
- Il cliente deve prevedere un'adeguata gestione delle autorizzazioni per far sì che al personale che utilizza o accede allo strumento vengano assegnati solo i diritti necessari per lo svolgimento della propria mansione lavorativa (principio del minimo privilegio).
- Impostare criteri password idonei conformi alle best practices e ai regolamenti vigenti.
- Preferire protocolli sicuri alle varianti non sicure, laddove supportati dallo strumento.
- A causa della mancata crittografia del traffico FTP da e verso lo strumento, si raccomanda di impostare e usare un utente dedicato per l'accesso ai dati tramite FTP.
- È necessario impostare processi e procedure per garantire che vengano utilizzate solo penne USB approvate e controllate, evitando l'uso di altre.
- È necessario disporre di processi e procedure per garantire l'adeguata gestione di audit trail, protocolli e dati di log in conformità con i regolamenti vigenti.
- Il personale deve ricevere una formazione in materia ddi sicurezza e sulle misure preventive di base.
- I processi e le procedure devono garantire l'esecuzione dei backup su base regolare e in conformità ai regolamenti vigenti.
- Il cliente è tenuto a garantire che non vengano usate informazioni sanitarie personali sullo strumento.

5 Software

5.1 Concetto di base

Il software in esecuzione sullo strumento è costituito dal software di base e da vari applicativi (indicati come processi applicativi). Il software di base rappresenta una piattaforma comune per tutti i programmi eseguibili, compresi i processi applicativi, gli strumenti e le impostazioni.

Processo applicativo

Un software indipendente rappresenta un processo biologico, ad es. il processo di trasduzione delle cellule T o l'arricchimento LP-34. Contiene una sequenza di fasi hardware e software predefinite per automatizzare il processo biologico. L'utente viene guidato passo dopo passo durante il processo. Esistono due tipi di processi applicativi:

- Processo applicativo standard: un processo applicativo prevalidato fornito di default.
- Processo applicativo personalizzato (CAP): un processo applicativo ad hoc sviluppato per clienti specifici.

Tool (Strumento)

Si tratta di un programma eseguibile svolge una funzione generica al di fuori di un processo applicativo come, ad esempio, controllare o modificare lo stato dell'hardware, trasferire dati, spegnere lo strumento ecc.

Setting (Impostazione)

È un programma eseguibile per configurare lo strumento come, ad esempio, Network Settings, Customer Settings e Module Settings

Per ogni programma eseguibile, verrà creata una cartella contenente tutte le informazioni. La cartella è denominata da
[Data] _ [Ora] _ [Numero di serie] _ [Programma eseguibile].

Il contenuto di questa cartella è controllato dal programma eseguito. Per i processi applicativi, i file rilevanti per il cliente sono elencati nella Tabella 5.1

Nome del file/ della cartella	Descrizione	Formatto
Protocol.pdf	Registrazione elettronica dell'esecuzione dell'applicazione	.pdf
Prototol_ Appendix_I.pdf	Registro degli errori e degli avvisi durante l'esecuzione dell'applicazione	.pdf
Interphase	Immagini della camera dello strato intermedio	Cartella
Microscope	Immagini al microscopio acquisite durante l'esecuzione dell'applicazione	Cartella
checksums.md5	Checksum	.md5
IR_Monitor	Registra l'ora e la temperatura quando la temperatura della superficie della camera risulta fuori specifica durante la coltura cellulare	.html

Tabella 5.1: Logfile dei processi applicativi

5.2 Interfaccia grafica utente

L'interfaccia grafica utente (GUI) contiene diverse sezioni: barra dei menu (con menu di accesso rapido), barra degli strumenti, barra di stato e area dei contenuti (Figura 5.1). Quando il software è in uso, gli elementi e i contenuti della GUI cambiano in base all'attività e al processo.

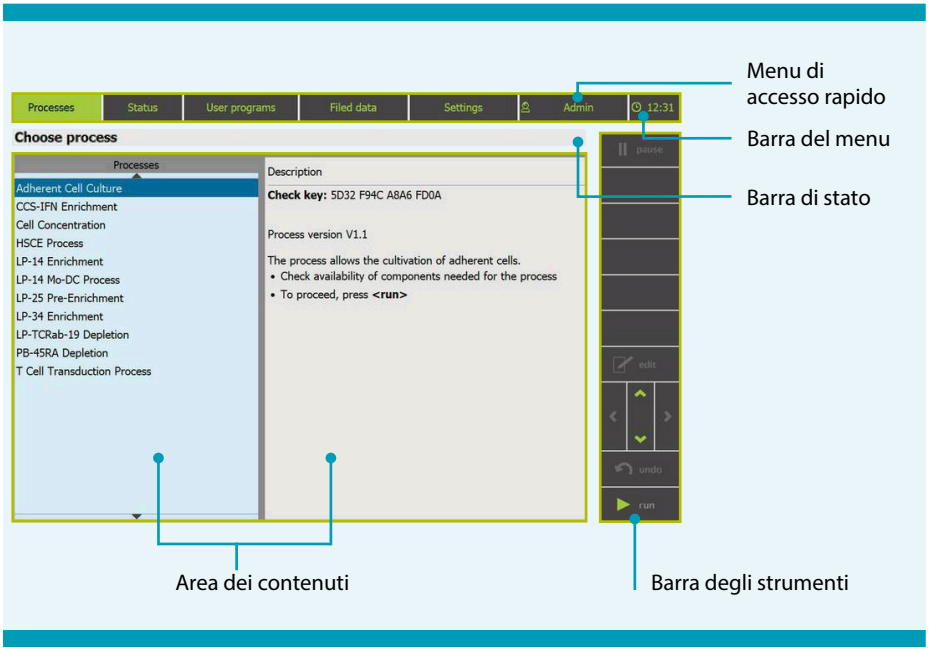


Figura 5.1: Sezioni dell'interfaccia grafica utente

5.2.1 Barra del menu e area dei contenuti

La barra del menu consente l'accesso a <Processes>, <Status>, <User Programs>, <Filed data>, <Settings> e (menu di accesso rapido). Uno sfondo verde indica quale pulsante del menu è attivo. Toccare l'area corrispondente per attivare il menu. L'area dei contenuti si adatta in base al menu selezionato. Dopo l'accesso, <Processes> (Processi) è selezionato di default e viene visualizzato il contenuto dei processi (vedere Figura 5.1).

Menu	Descrizione
<Processes> (Processi)	Accesso ai processi applicativi standard installati sugli strumenti (Schermata 6.5) e guida all'esecuzione dei processi (Schermata 6.6)
<Status> (Stato)	Stato dello strumento durante l'esecuzione di un processo applicativo (Figura 6.1)
<User Programs> (Programmi utilizzatore)	Accesso al processo applicativo personalizzato (CAP) di Miltenyi Biotec e guide all'esecuzione del processo
<Filed data> (Dati archivati)	Accesso alla visualizzazione e all'esportazione dei dati generati da processi, strumenti e impostazioni (Schermata 7.1).
<Settings> (Impostazioni)	Accesso alle impostazioni e agli strumenti per la configurazione dello strumento, il test di funzionamento e la risoluzione dei problemi di base (Schermata 8.1)
Menu di accesso rapido	Accesso a Logout, User Management, criteri password, Audit Trail e pulsante Shutdown (Schermata 6.3)
System time (Ora di sistema)	Ora corrente del sistema.

Tabella 5.2: I menu nella barra del menu

5.2.2 Barra di stato

La barra di stato (vedere Figura 5.1) contiene brevi informazioni sullo stato del processo in corso.

5.2.3 Barra degli strumenti

La barra degli strumenti contiene vari pulsanti per controllare il processo. La disponibilità dei pulsanti e il loro stato attivo sono controllati dal processo applicativo. Nella Figura 5.2 sono riportati esempi di barre degli strumenti durante due diversi processi applicativi. Il colore verde indica uno stato 'attivo', il colore grigio indica uno stato 'inattivo'.
I pulsanti utilizzati di frequente sono descritti nella Tabella 5.3.



Figura 5.2: Tasti dinamici e statici della barra degli strumenti

Nome tasto	Descrizione	Disponibilità
<pause>	arresto/sospensione temporanea del processo in esecuzione, dipende dall'applicazione in esecuzione	durante l'esecuzione di un processo
<edit>	attiva il campo di inserimento di dati manuali (vedere 5.2.4 ´Campi di inserimento´).	se i campi di inserimento sono disponibili
tasti di navigazione	per selezionare elementi da un elenco: utilizzare ^ v per spostare l'elemento selezionato in alto e in basso nell'elenco (vedere Schermata 6.5) o < > per passare da un elenco all'altro (vedere Schermata 8.1). per navigare nelle immagini della camera (Figura 6.3).	sempre se la camera è attiva
<undo>	revoca uno o più inserimenti per ripristinare il contenuto originale dello schermo	durante l'esecuzione di un processo
<ok>/<run>	<ok> conferma una selezione o chiude il menu attivo <run> avvia un processo, un programma utente o qualsiasi altra procedura	sempre

Tabella 5.3: Pulsanti più frequenti della barra degli strumenti

5.2.4 Campi di inserimento

Un campo di inserimento rappresenta una tastiera e consente l'immissione di lettere o numeri (vedere Figura 5.3). Per l'inserimento manuale delle lettere maiuscole, toccare <⇧>, per lo spazio toccare <SP>, per i numeri toccare <?123> e per eliminare il carattere che precede il cursore o il testo selezionato toccare <⌫>. Per aprire i campi di inserimento, toccare <edit> nella barra degli strumenti. Per chiudere il campo di inserimento, toccare <ok> sotto i campi di inserimento per confermare l'inserimento o toccare <Escape> in alto a destra per chiudere senza salvare.

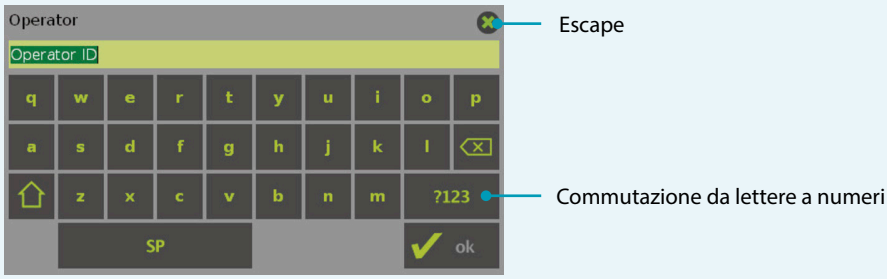
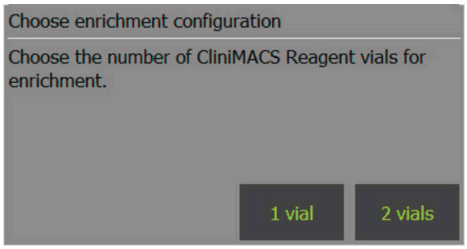


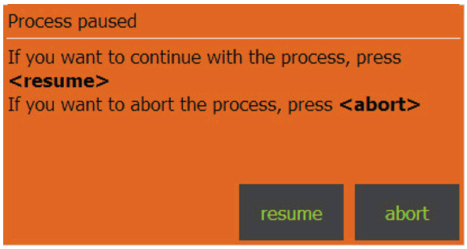
Figura 5.3: Il campo di inserimento – tastiera con lettere

5.2.5 Finestre pop-up

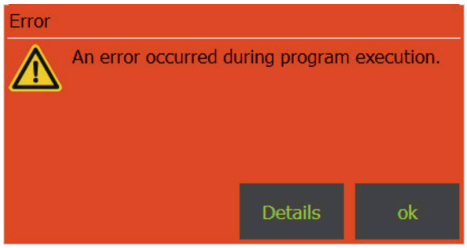
Durante l'esecuzione di programmi eseguibili potrebbero comparire finestre pop-up. Il processo in esecuzione verrà interrotto fino a che la finestra pop-up non viene chiusa. Se necessario, è possibile trascinare le finestre pop-up sullo schermo tenendo premuta la barra superiore. Una finestra pop-up viene visualizzata in diversi casi:



Sono necessari un inserimento o una conferma. La finestra pop-up ha uno sfondo grigio. Selezionare uno dei pulsanti per continuare il processo.



È necessario confermare un avviso dello strumento o una decisione importante. La finestra pop-up ha uno sfondo arancione. Selezionare uno dei pulsanti per prendere una decisione.



Si è verificato un errore. La finestra pop-up ha uno sfondo rosso. Selezionare uno dei pulsanti in basso per continuare.

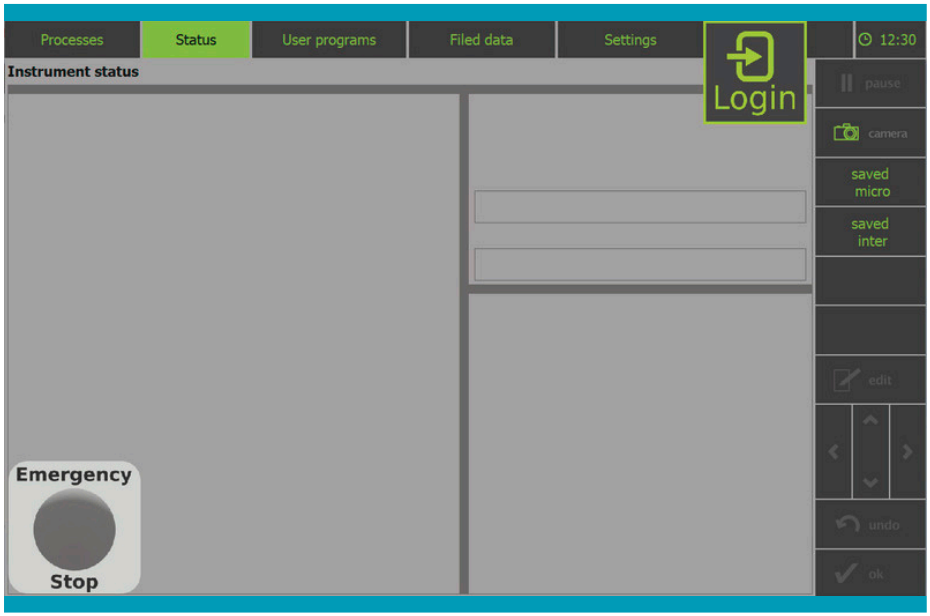
Se necessario, contattare Miltenyi Biotec Technical Support

6

Operazioni di base

6.1 Accendere lo strumento

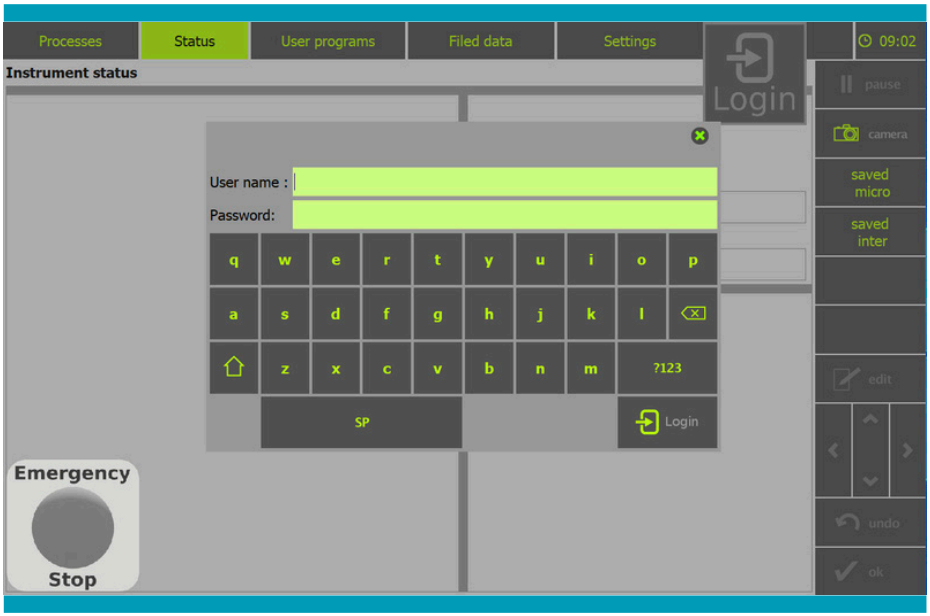
Accendere CliniMACS Prodigy utilizzando l'interruttore di alimentazione sul retro dello strumento. La schermata iniziale mostra la versione del software e per un breve istante (ca. 5 secondi) viene visualizzato il processo di inizializzazione. Dopo il processo di inizializzazione, apparirà una schermata di blocco (vedere Schermata 6.1). In questa schermata è attivo solo il pulsante **<Login>**.



Schermata 6.1: Schermata di blocco

6.2 Login

Toccare <Login> nell'angolo in alto a destra della schermata per aprire la finestra pop-up <User Login> (vedere Schermata 6.2). Inserire nome utente e password e toccare <Login> nella finestra pop-up. La schermata viene sbloccata. Il nome utente e la password devono essere impostati prima dell'uso (vedere capitolo 10 ´Gestione degli utenti´ per i dettagli).



Schermata 6.2: Finestra di login per l'utente

Nota: se non è possibile effettuare il login, contattare un amministratore di sistema per verificare:

- se il nome utente e la password siano corretti.
- di quali diritti di accesso disponga l'account. Per maggiori informazioni, vedere il capitolo 10 'Gestione degli utenti'.

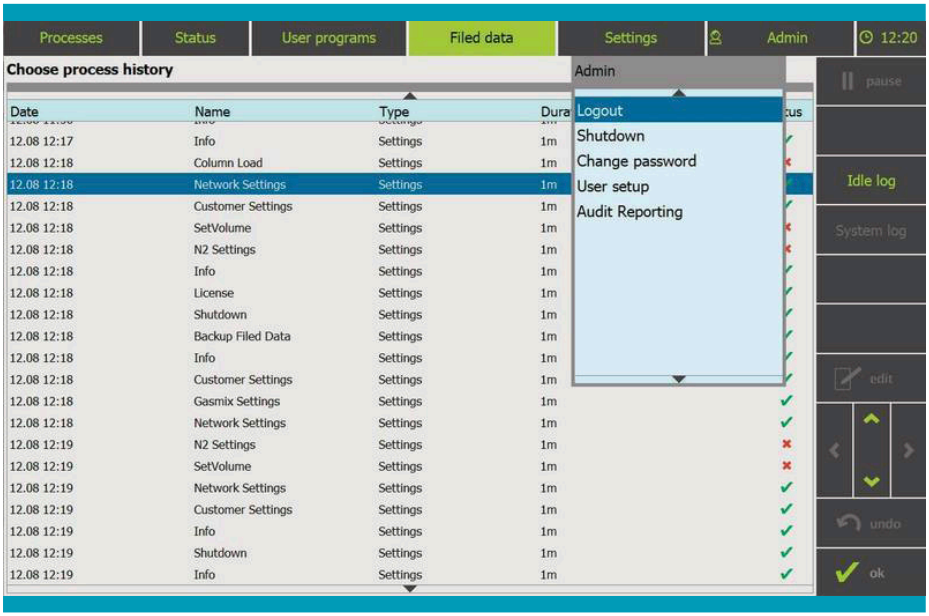
Se durante il login compare una notifica pop-up non correlata a credenziali dell'utente errate né a diritti di accesso insufficienti, toccare <ok>. Successivamente, inserire nuovamente le credenziali dell'utente.

Se il problema persiste, contattare il Miltenyi Biotec Technical Support.

6.3 Logout

Toccare (menu di accesso rapido) e selezionare <Logout> dall'elenco (vedere Schermata 6.3). La schermata risulterà quindi bloccata di nuovo.

Nota: dopo 20 minuti senza interazione con il software, l'utente verrà disconnesso automaticamente.



Schermata 6.3: Logout

6.4 Shutdown (Spegnimento

Toccare (menu di accesso rapido). Selezionare <Shutdown> dall'elenco (vedere Schermata 6.3). In alternativa, selezionare <Settings> ▸ <Tools> ▸ <Shutdown>. Attendere che il processo di spegnimento abbia termine, quindi spegnere lo strumento utilizzando l'interruttore di alimentazione sul retro.

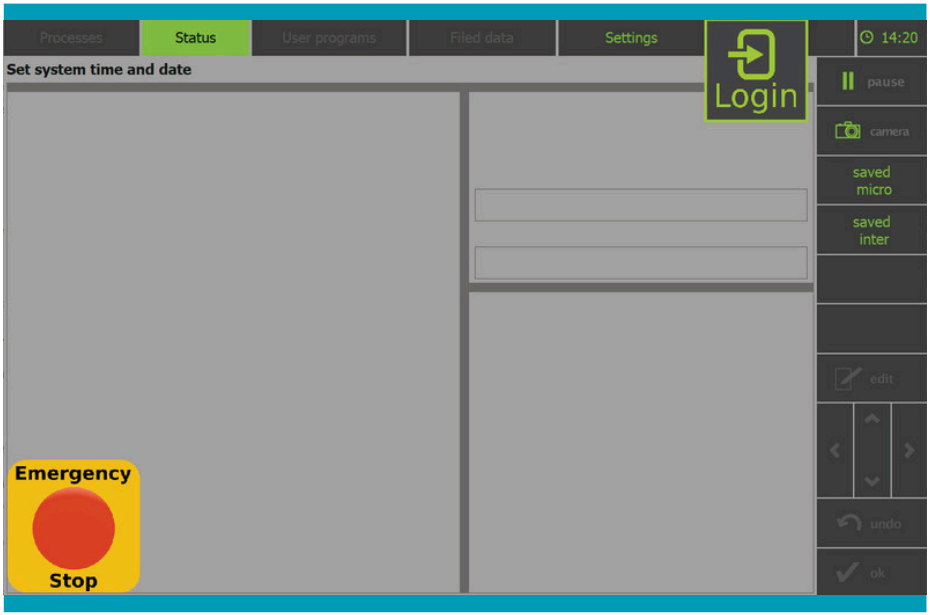
6.5 Emergency Stop

<Emergency Stop> consente di mettere in pausa l'applicazione o lo strumento attualmente in uso in caso di emergenza, senza la necessità di effettuare il login preventivamente. Per soddisfare i requisiti del 21 CFR Parte 11, è necessario effettuare un successivo login e inserire il motivo dell'arresto di emergenza. Il pulsante <Emergency Stop> è attivato (indicato dai colori giallo e rosso) solo quando un'applicazione o uno strumento sono in esecuzione e nessun utente è connesso (vedere Schermata 6.4).

IMPORTANTE

L'arresto di emergenza <Emergency Stop> non spegne completamente lo strumento, ma ha la stessa funzione del tasto <pause> durante un'applicazione in esecuzione quando un utilizzatore è connesso.

Per riprendere l'applicazione, l'utilizzatore che dispone dei diritti per l'applicazione deve effettuare il login.

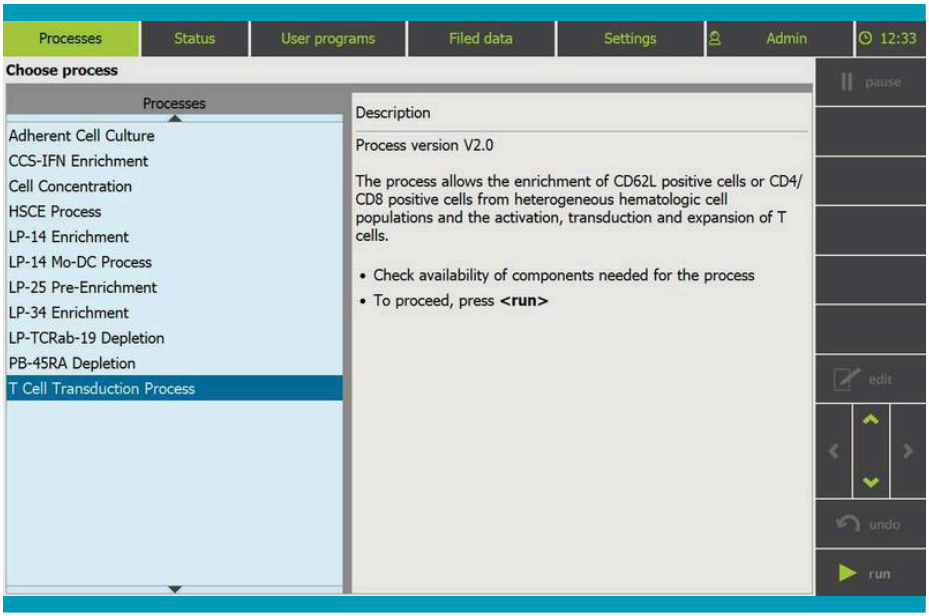


Schermata 6.4: Pulsante Emergency Stop

6.6 Selezionare un processo applicativo

1. Toccare <Processes> (Processi) nella barra dei menu, per selezionare un processo applicativo standard. Per un CAP toccare <User Programs>.
2. Selezionare il processo desiderato dall'elenco dei processi (Schermata 6.5). Il processo selezionato è evidenziato con uno sfondo blu. La descrizione dell'applicazione è riportata a destra. Toccare nell'elenco dei processi o utilizzare ^ e ˇ nella barra degli strumenti per navigare tra i processi disponibili.

Nota: il contenuto nell'elenco dei processi varia in base al ruolo e ai diritti dell'utente corrente. Un'applicazione viene visualizzata solo se l'utente correntemente connesso dispone dei diritti di accesso. Per ulteriori informazioni su ruoli e diritti vedere il capitolo 10 ´Gestione degli utenti´.



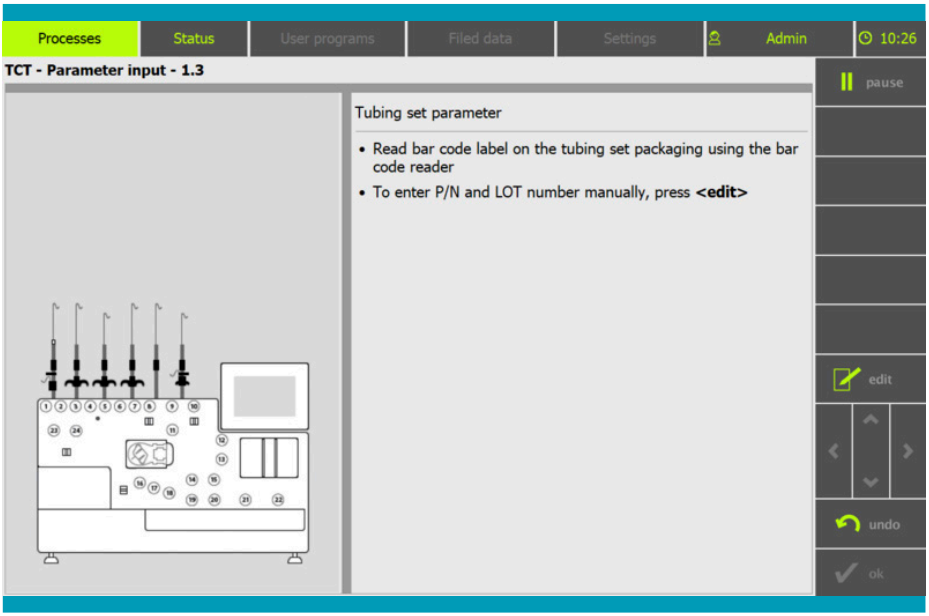
Schermata 6.5: Selezionare un processo applicativo

6.7 Eseguire un processo applicativo

Per avviare un processo, selezionarlo e toccare **<run>** nella barra degli strumenti. Il software fornisce una guida dettagliata al processo.
Schermata 6.6 fornisce un esempio di fase dell'applicazione TCT. La barra di stato mostra il nome e l'indice della fase corrente. L'area dei contenuti fornisce ulteriori informazioni sulla fase in corso. Seguire l'illustrazione e le istruzioni riportate nell'area dei contenuti per ciascun passaggio.

In alcuni passaggi del processamento è necessario l'input dell'utente. Tra le informazioni tipicamente richieste vi sono il codice del componente (P/N), il numero di LOTTO e i valori misurati. Il codice del componente e il numero di LOTTO possono essere inseriti mediante lo scanner di codici a barre o manualmente. Per l'inserimento manuale o se l'immissione tramite scanner di codici a barre non è accettata, toccare **<edit>** nella barra degli strumenti e utilizzare il campo di inserimento.

Una volta completate tutte le azioni necessarie, **<ok>** nella barra degli strumenti sarà abilitato. Per passare alla fase successiva, toccare **<ok>**. Per tornare alla fase precedente, toccare **<undo>**.



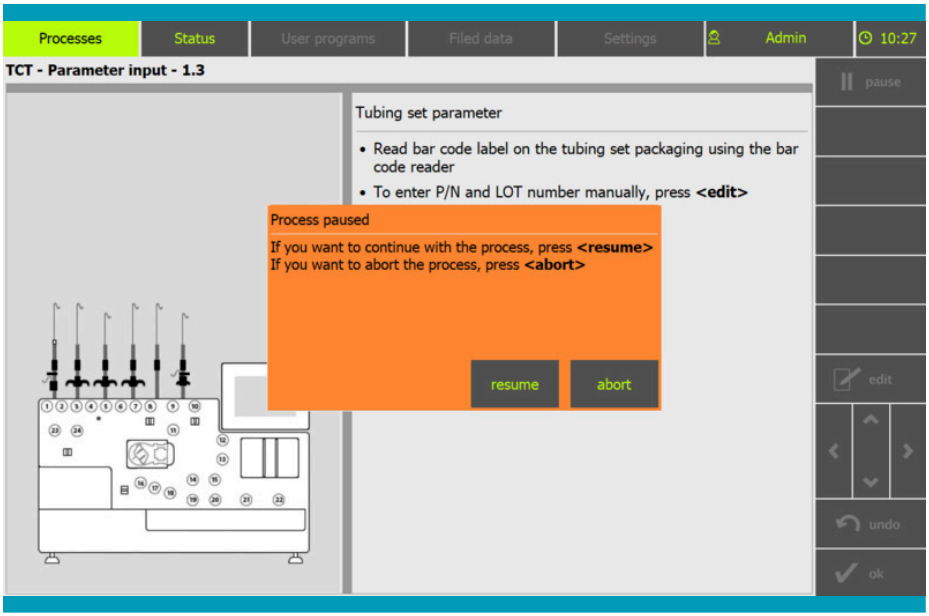
Schermata 6.6: Esempio di fase nel processo applicativo TCT

6.8 Sospendere un processo applicativo

Per sospendere il processo in corso, toccare **<pause>** nella barra degli strumenti. Viene visualizzata una finestra pop-up (Schermata 6.7). Per continuare un processo sospeso, toccare **<resume>**. Per terminare il processo, toccare **<abort>**.

IMPORTANTE

Non è possibile riprendere un processo interrotto.



Schermata 6.7: Processo sospeso

6.9 Stato dello strumento e del processo applicativo

Per controllare lo stato operativo del processo in esecuzione, toccare <Status> nella barra dei menu. Nell'area dei contenuti sono presenti i seguenti elementi:

- Parametro relativo al processo: un elenco di tutti i parametri di processo rilevanti (vedere Figura 6.1, a sinistra).
- Riquadro con le informazioni e lo stato di avanzamento: informazioni relative al processo (vedere Figura 6.1, in alto a destra):
  - Nome dell'operatore
  - Informazioni sul campione
  - Avanzamento del sottoprocesso e tempo rimanente
  - Avanzamento del processo e tempo rimanente prima della successiva interazione con l'utente
- Panoramica grafica: fornisce informazioni visive sullo stato dei sottoprocessi in esecuzione dello strumento (vedere Figura 6.1, in basso a destra). Tutte le attività dei componenti dello strumento (ad es. pompa peristaltica, valvole a pinza) sono visualizzate in arancione.

Nota: le informazioni sullo stato sono disponibili solo durante l'esecuzione di un'applicazione. Se non vi sono applicazioni in esecuzione, questa pagina è vuota. La panoramica grafica potrebbe non essere disponibile per i CAP.

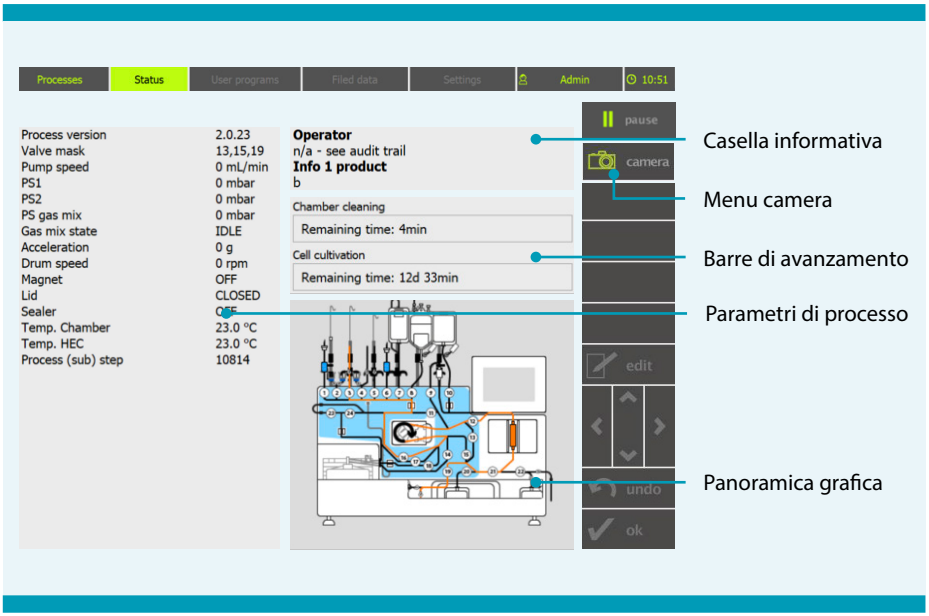


Figura 6.1: Panoramica dello stato dello strumento

6.10 Acquisizione di immagini

Durante applicazioni selezionate, <camera> nella barra degli strumenti consente di selezionare due funzionalità (vedere Figura 6.1).

- Immagine della camera di rilevazione strati: questa immagine viene utilizzata per misurare i volumi delle frazioni di centrifugazione. È disponibile solo in e per applicazioni selezionate e durante la prima regolazione del volume dopo il caricamento del campione (vedere Figura 6.2).
- Immagine al microscopio: questa immagine può essere utilizzata per monitorare visivamente la coltura cellulare. È disponibile solo durante procedure di coltura cellulare (vedere Figura 6.3).

L'immagine verrà automaticamente acquisita e salvata nel protocollo dal processo applicativo. Per visualizzare le immagini, toccare <camera> nella barra degli strumenti quando è selezionato il menu <Status> (vedere Figura 6.1). A seconda della fase del processo applicativo, l'area dei contenuti mostrerà l'immagine della camera di rilevazione strati o l'immagine al microscopio.

Nota: la disponibilità di <camera> nella barra degli strumenti è controllata dal processo applicativo. Le immagini verranno registrate automaticamente durante un'applicazione.

6.10.1 Camera di rilevazione strati

I differenti strati vengono rilevati automaticamente dal software. Nella Figura 6.2 le barre rossa e arancione segnano la posizione dei livelli all'interno dell'immagine. Un diagramma sotto l'immagine visualizza i valori registrati per i volumi delle frazioni di centrifugazione. Le curve sono visualizzate in rosso e arancione corrispondenti alle barre all'interno dell'immagine (vedere Figura 6.2).

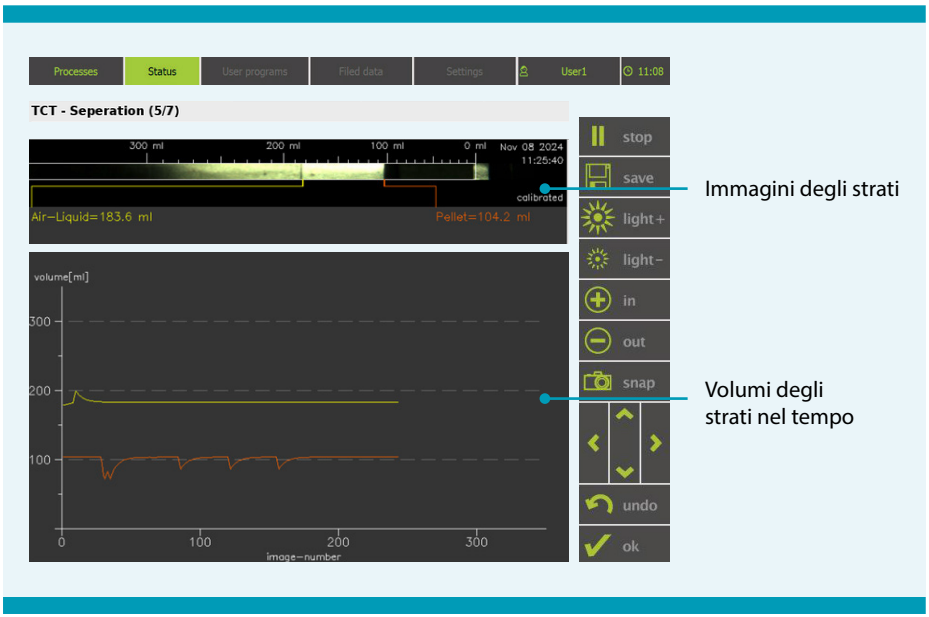


Figura 6.2: Panoramica dello stato dello strumento

Sono supportate le seguenti funzionalità:

- Acquisizione di immagini: toccare <snap> nella barra degli strumenti. Dopo una breve fase di registrazione (circa 15 secondi), l'immagine visualizzata viene sostituita da una nuova immagine registrata.
- Archiviazione di immagini: toccare <save> nella barra degli strumenti. L'immagine registrata viene integrata nel protocollo del processo attuale.
- Uscire dal menu camera: toccare <ok> nella barra degli strumenti.

Nota: la disponibilità dei pulsanti precedenti è controllata dal processo applicativo.

6.10.2 Camera con microscopio

Il menu camera mostra l'ultima immagine salvata dalla camera integrata del microscopio (vedere Figura 6.3).

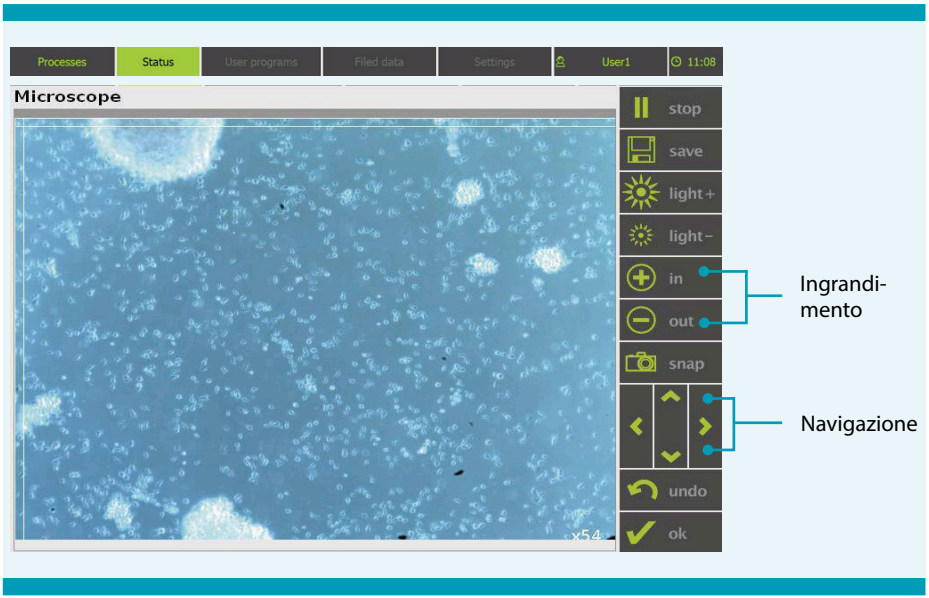


Figura 6.3: Schermo di stato quando la camera con microscopio è attiva

Sono supportate le seguenti funzionalità:

- Ingrandire l'immagine: Toccando l'immagine della camera con microscopio si ottiene un ingrandimento di 2 volte. Il punto toccato sarà il nuovo centro dell'immagine. L'ingrandimento delle immagini è fino a 400×.
- Navigazione all'interno di un'immagine: Premendo un tasto di navigazione si ottiene uno spostamento di metà fotogramma nella direzione selezionata. Le barre di scorrimento dell'immagine indicano la posizione assoluta della sezione di immagine all'interno della stessa per facilitare la navigazione. Toccare ripetutamente **<undo>** per annullare separatamente gli ultimi dieci operazioni di navigazione.
- Acquisizione di immagini: toccare **<snap>** nella barra degli strumenti. Dopo una breve fase di registrazione (circa 15 secondi), l'immagine visualizzata viene sostituita da una nuova immagine registrata.
- Archiviazione di immagini: toccare **<save>** nella barra degli strumenti. L'immagine registrata viene integrata nel protocollo del processo attuale.
- Uscire dal menu camera: per uscire dal menu camera toccare **<ok>** nella barra degli strumenti.

Nota: la disponibilità dei pulsanti precedenti è controllata dal processo applicativo.

7 Accesso ai dati

7.1 Recupero dei log delle applicazioni

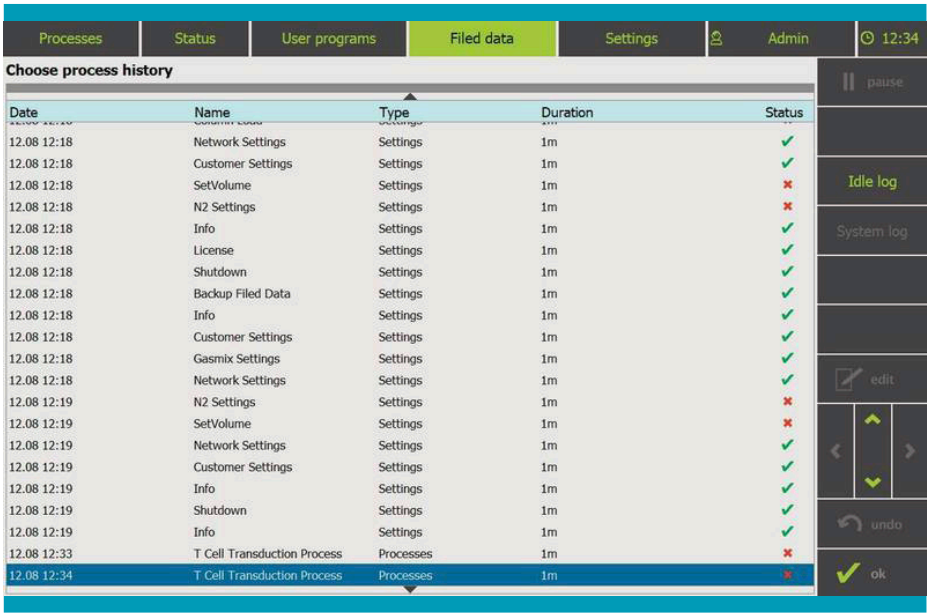
7.1.1 Visualizzazione ed esportazione dei logfile su USB

Il menu <Filed data> mostra il logfile generato dai processi applicativi, dagli strumenti e dalle impostazioni. Nell'area dei contenuti, l'elenco dei file mostra l'ora, il nome, il tipo, la durata e lo stato di esecuzione del processo (Schermata 7.1).

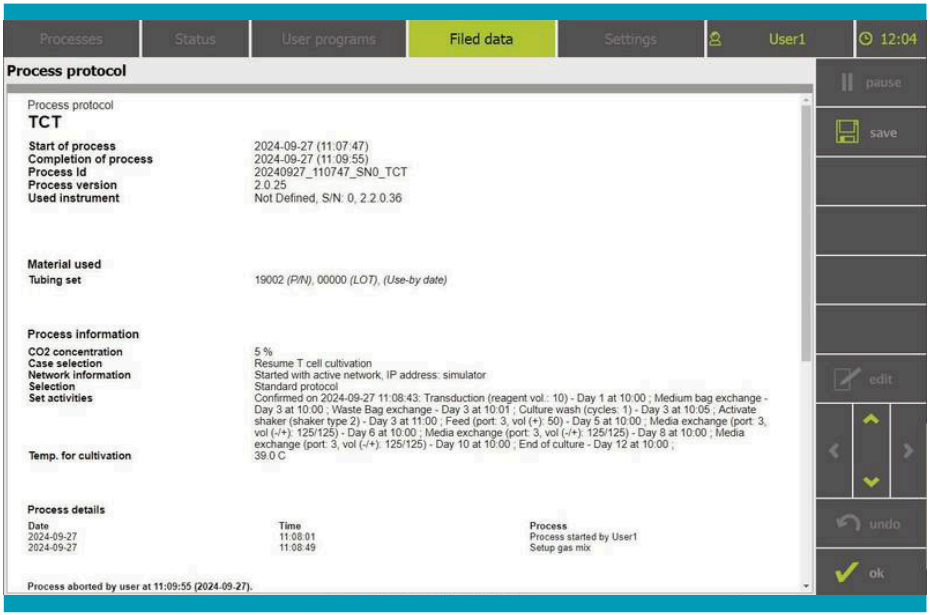
Nota: il menu <Filed data> non è disponibile durante l'esecuzione di un processo. Il corrispondente pulsante a sfioramento è inattivo.

Visualizzazione dei logfile

Per visualizzare il contenuto del PDF del protocollo di processo e dell'appendice del protocollo, selezionare il logfile desiderato e toccare <ok> (vedere Schermata 7.1). Il contenuto del file selezionato viene visualizzato nell'area dei contenuti (vedere Schermata 7.2). Per tornare all'elenco dei file toccare <ok>.



Schermata 7.1: Esempio di elenco di dati archivio



Schermata 7.2: Esempio di protocollo di processo (applicazione TCT)

Esportazione su penna USB

1. Inserire una penna USB.
2. Aprire il logfile di destinazione e toccare **<save>** nella barra degli strumenti.

IMPORTANTE

- Assicurarsi che il nome della penna USB non sia 'netext', poiché questo termine è riservato al software.
- Per eseguire il backup di tutti i dati del processo, è possibile usare lo strumento Backup Filed Data, vedere sezione 8.2.2 ´Backup Filed Data´.
- La penna USB deve essere in formato FAT32 e non deve essere protetta da password.

7.1.2 Recupero tramite FTP

FTP è un protocollo di rete che consente il trasferimento di dati tra CliniMACS Prodigy (definito server FTP) e il computer dell'utente finale (definito client FTP) attraverso connessioni IP (Internet Protocol). È possibile accedere a tutti i logfile generati dall'esecuzione dell'applicazione.

Per accedere ai dati tramite FTP, è necessario procedere a una configurazione. Per configurare lo strumento per la connessione FTP, seguire le istruzioni riportate nella sezione 9.4.1 ´Configurazione dello strumento´. Completata la configurazione, l'utente può effettuare la connessione allo strumento con qualsiasi client FTP disponibile (ad es. FileZilla) per scaricare protocolli e logfile, Figura 7.1 mostra un esempio di parametri di connessione. Per la connessione allo strumento, inserire le seguenti informazioni:

- L'indirizzo IP dello strumento, che si trova in **<Settings>** ▸ **<Tools>** ▸ **<Info>** ▸ **<Network information>**.
- Ingresso: usare la porta standard 21.
- Per il nome utente e la password sono supportate due opzioni di login:
  - Opzione di login 1: un account registrato nel sistema di gestione degli utenti (vedere capitolo 10 ´Gestione degli utenti´). In questo caso, si usano l'account e la password di accesso dell'utente. L'avvio e la chiusura della connessione saranno registrate nell'audit trail.
  - Opzione di login 2: un nome utente e una password locali salvati in FTP/File Share Settings. Le informazioni di login si trovano in **<Settings>** ▸ **<Network Settings>** FTP/FS. In questo caso, l'avvio e la chiusura della connessione non saranno registrate nell'audit trail.

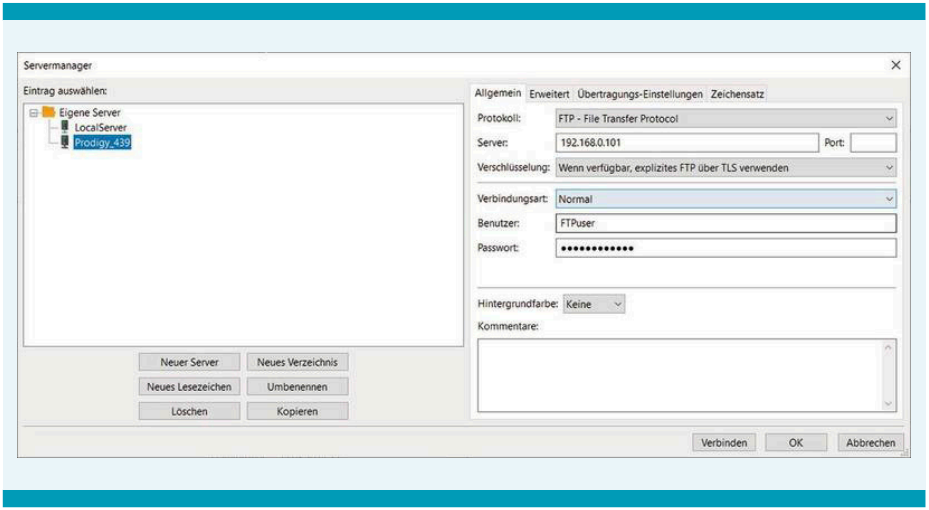


Figura 7.1: Parametri di connessione esemplificativi

- **IMPORTANTE**
  Se si utilizza l'opzione di accesso 1, assicurarsi che il ruolo 'File management user' sia assegnato a questo account. Per la modalità di assegnazione del ruolo all'account, consultare il capitolo 10 'Gestione degli utenti'.
- Il software non supporta un FTP sicuro (sFTP). Se si accede ai file tramite FTP, si raccomanda di utilizzare lo strumento in una rete isolata .

Nota: un singolo utente può stabilire una sola connessione alla volta, poiché il server dello strumento non consente connessioni multiple. Con software client che utilizza connessioni simultanee (ad es. FileZilla), occorre modificare le impostazioni del client in modo da consentire solo una singola sessione. In caso contrario, sarà possibile sfogliare i contenuti ma non scaricarli.

7.1.3 Recuperare i file tramite la condivisione di file

I logfile generati durante l'esecuzione dell'applicazione possono essere recuperati tramite una cartella di rete condivisa. Una volta completata l'esecuzione dell'applicazione, tutti i file generati verranno automaticamente inseriti in una sottocartella creata per ciascun strumento all'interno della cartella condivisa. Figura 7.2 mostra la struttura dei file nella cartella condivisa. Per abilitare la condivisione di file, è necessario procedere a una configurazione. Per impostare la condivisione di file, seguire le istruzioni riportate Nella sezione 9.3 ´Connessione a un drive di rete´.

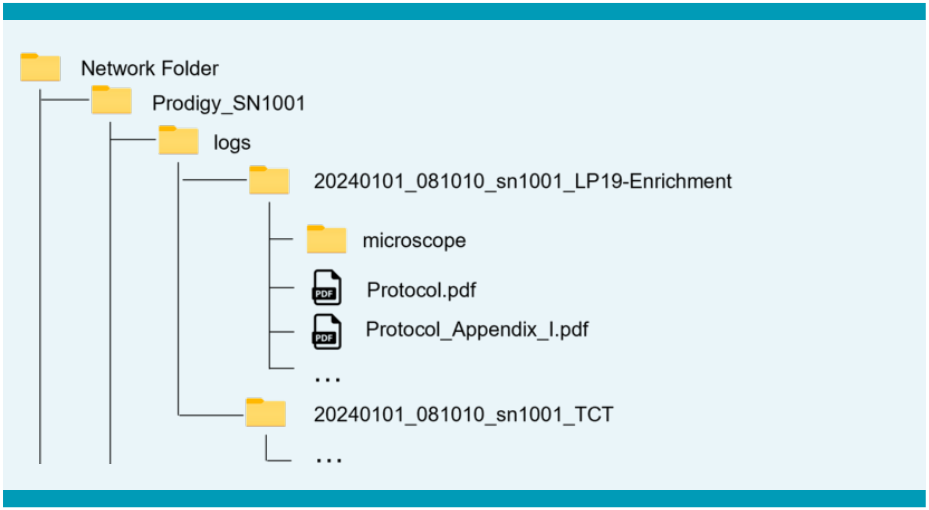


Figura 7.2: Struttura dei file nella condivisione di file

IMPORTANTE

I logfile memorizzati sullo strumento sono protetti da un controllo degli accessi in modo di consentire l'accesso solo al personale autorizzato. Una volta che questi file vengono trasferiti su un'unità di rete, l'utente ha la responsabilità di implementare adeguate misure di controllo degli accessi.

7.2 Recupero di audit trail

Il sistema di audit trail registra tutte le interazioni dell'utente con il software. Ogni interazione con l'utente dà luogo a un record audit trail con l'utente che ha eseguito l'azione, il timestamp e la descrizione dell'interazione. L'audit trail può essere esportato in formato .pdf e .csv. La Tabella 7.1 mostra il formato audit trail.

IMPORTANTE

Il timestamp del record audit trail è sempre nel fuso orario UTC.

Ora	Categoria	Tipo	User	Descrizione
2020-Jul-21 10:33:44	Interazione utente	Chiusura pop-up	ID account	'Avviso' Avanzamento sospeso
...	...	...	...	...

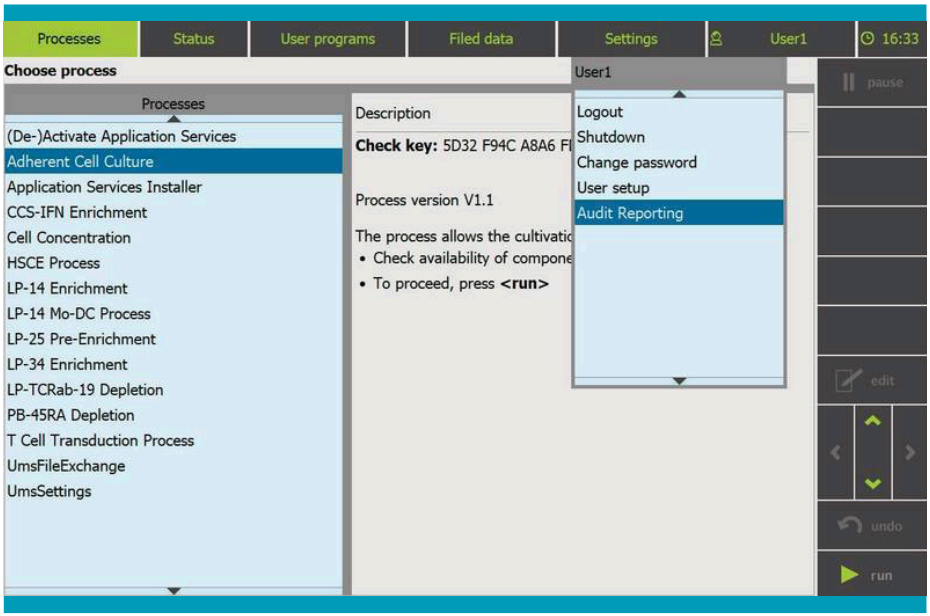
Tabella 7.1: Formato audit trail

Nota: per accedere al sistema di audit trail è necessario il ruolo 'ATS User' o un ruolo con diritti 'Audit Trail Management'.

- Il ruolo 'ATS User' ha un accesso completo che consente di visualizzare, esportare ed eliminare i record audit trail.
- È possibile creare un nuovo ruolo per l'accesso limitato alle funzioni di audit trail. Per maggiori dettagli su come configurare ruoli e diritti, vedere il capitolo 10 'Gestione degli utenti'.

7.2.1 Visualizzazione di audit trail

Per aprire Audit trail, selezionare ▸ <Audit Reporting> (vedere Schermata 7.3). Il menu <Audit Trail> contiene un elenco di tutti gli eventi audit trail disponibili sullo strumento (vedere Figura 4.1).



Schermata 7.3: Report di audit trail

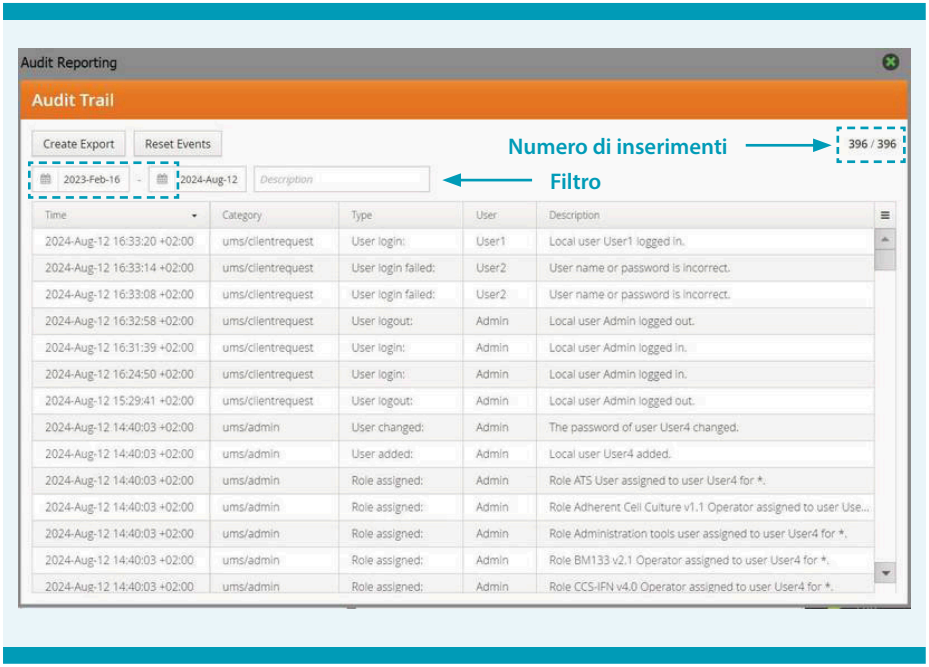
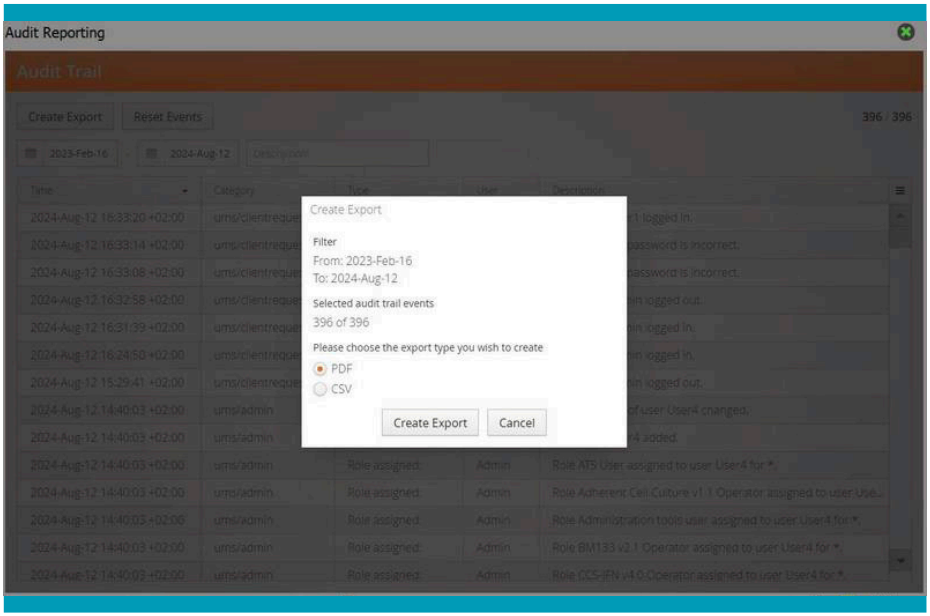


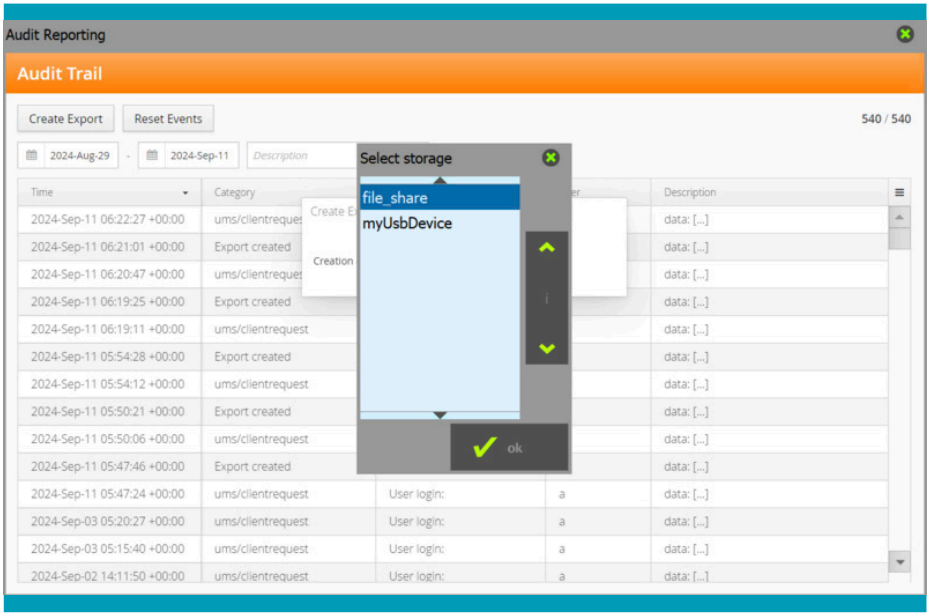
Figura 7.3: Menu Audit trail

7.2.2 Esportazione di audit trail

1. Inserire i criteri di filtro nei campi mostrati nella Figura 7.3. Se non viene inserito alcun criterio, vengono esportati tutti i record audit trail.
2. Toccare **<Create Export>** sopra i criteri di filtro. Viene visualizzata una finestra pop-up (Schermata 7.4).
3. Scegliere il formato e toccare **<Create Export>** nella finestra pop-up.
4. Se vengono rilevate più posizioni di archiviazione, ad es. se è stata configurata la condivisione di file e viene inserita una penna USB, è necessario scegliere la posizione di archiviazione (Schermata 7.5).



Schermata 7.4: Creare l'esportazione di audit trail



Schermata 7.5: Selezionare la posizione di archiviazione per l'audit trail

5. Attendere il completamento del processo e verificare che il file sia stato esportato.

7.2.3 Eliminazione di audit trail

1. Per eliminare tutte le voci audit trail, toccare **< Reset Events >** (Reimposta eventi).

2. Confermare con **<Continue Reset>**. Dopo il ripristino, tutti i record vengono eliminati. Viene aggiunto un nuovo record per l'azione di eliminazione.

IMPORTANTE

Non è possibile eliminare singole voci. I dati eliminati non possono essere ripristinati. Assicurarsi che solo gli utenti autorizzati dispongano del diritto di eliminare l'audit trail. Per configurare ruoli e diritti, vedere il capitolo 10 'Gestione degli utenti'.

8

Strumenti e impostazioni utente

8.1 Accesso agli strumenti e alle impostazioni utente

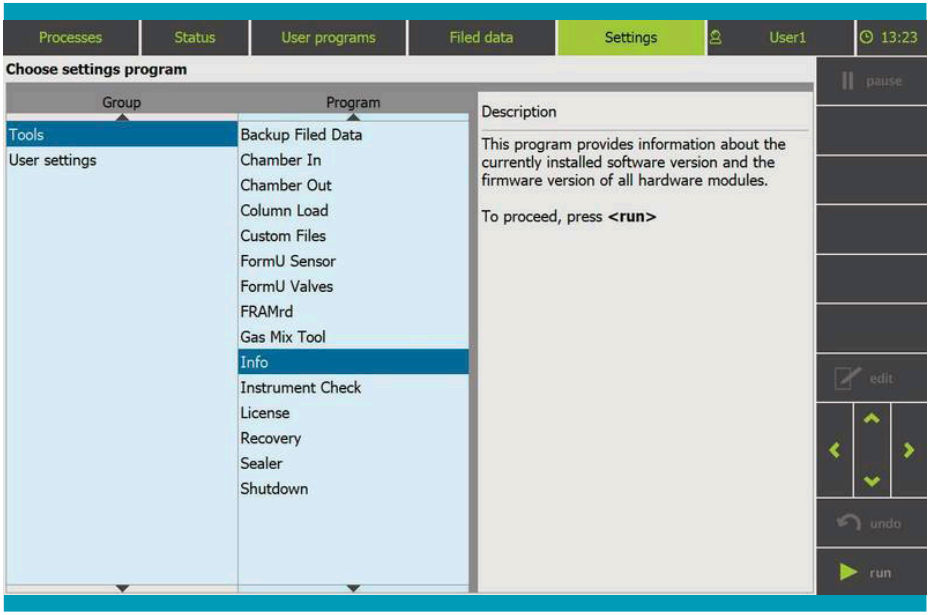
Nel menu <Settings> si trovano due tipi di programmi: Tools (strumenti) e Settings (impostazioni).

Nota: durante l'esecuzione di un processo, gli strumenti e le impostazioni non sono disponibili.

Per trovare ed eseguire uno strumento/un'impostazione:

1. Selezionare <Tools> o <User settings> dall'elenco Group, vediSchermata 8.1.
2. Nell'elenco dei programmi, toccare il programma desiderato. Il programma selezionato è evidenziato con uno sfondo blu. Nel campo Description sono riportate informazioni dettagliate su strumento/impostazione selezionati. Per sfogliare altre opzioni, toccare ^ e v nell'elenco dei processi. In alternativa, utilizzare i pulsanti di navigazione per sfogliare e selezionare il programma.
3. Per avviare il programma selezionato, toccare <run> nella barra degli strumenti.

Nelle sezioni seguenti vengono presentati gli strumenti e le impostazioni utente più comuni.



Schermata 8.1: Selezionare uno strumento o un'impostazione

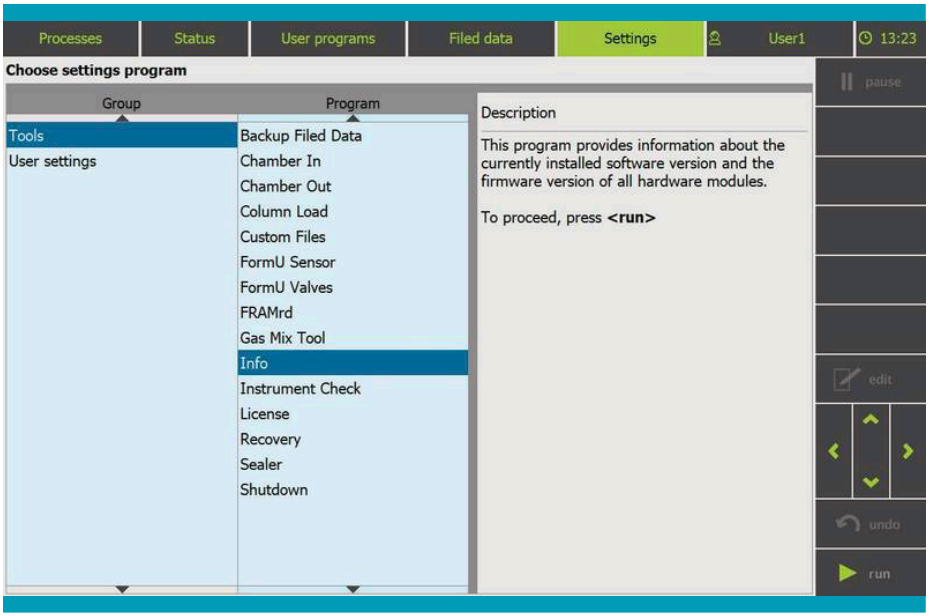
8.2 Tools (Strumenti)

Tutti gli strumenti si trovano in <Settings> ▸ <Tools>.

8.2.1 Info tool (Strumento Info)

Lo strumento Info fornisce informazioni dettagliate su software e hardware. Le informazioni importanti includono:

- Versione del software
- Numero di build
- Versione del firmware
- Utilizzo dello spazio sul disco rigido, compreso lo spazio rimanente, lo spazio utilizzato e lo spazio totale
- Indirizzo IP
- Indirizzo MAC
- Informazioni complete sul tempo di esecuzione (incluse tutte le applicazioni e gli strumenti), tempo di inattività (tempo in cui lo strumento non eseguiva alcuna applicazione)



Schermata 8.2: Info tool (Strumento Info)

8.2.2 Backup Filed Data

Lo strumento Backup Filed Data copia tutti i dati del processo in una posizione di backup o elimina tutti i dati del processo.

IMPORTANTE

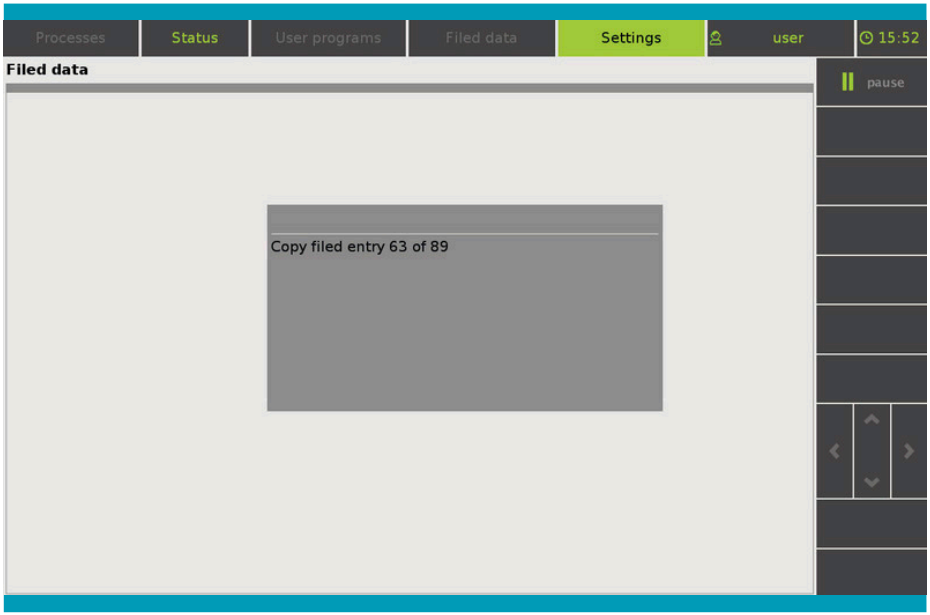
- Si consiglia di eseguire regolarmente il backup dei dati di processo. In caso contrario, potrebbe apparire un messaggio che avvisa l'utente che il programma non può essere avviato perché è stato raggiunto il limite massimo di dati archiviati.
- Se si utilizza una penna USB per il backup, questa deve essere in formato FAT32 e non deve essere protetta da password.
- Se la condivisione dei file è configurata, i file possono essere esportati anche nella cartella di condivisione dei file (vedere sezione 9.3 ´Connessione a un drive di rete´).

Copiare dati

1. Inserire una penna USB.
2. Selezionare <Settings > ▸ <Tools> ▸ <Backup Filed Data>, e toccare <run>.
3. Selezionare <Backup> nella finestra di dialogo (vedere Schermata 8.3). L'operazione di copia viene avviata (vedere Schermata 8.4).

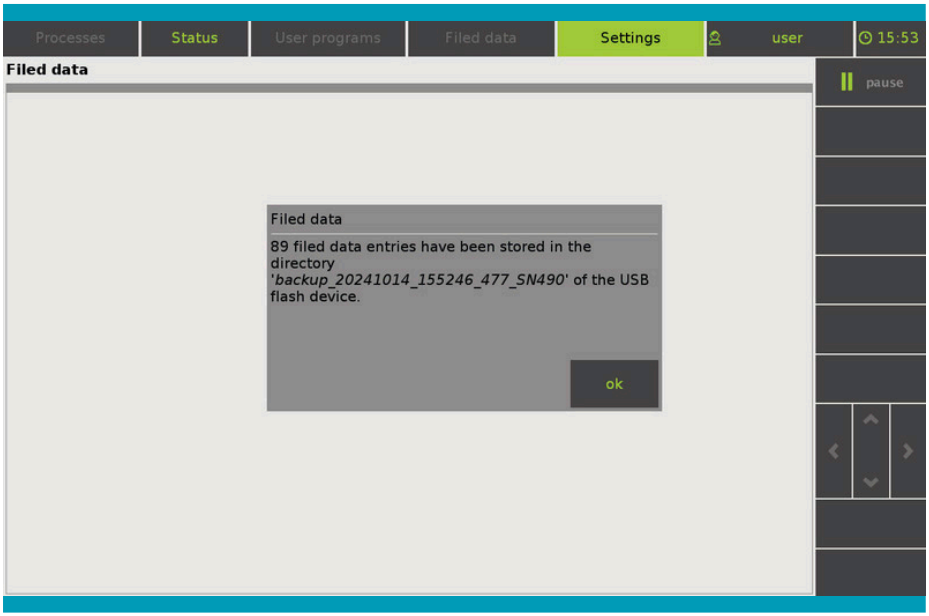


Schermata 8.3: Selezionare backup



Schermata 8.4: Processo di backup

4. Attendere che l'operazione di copia sia conclusa, quindi toccare <ok> nella finestra di dialogo (vedere Schermata 8.5).
5. Verificare che i file siano stati scaricati completamente.



Schermata 8.5: Backup completato

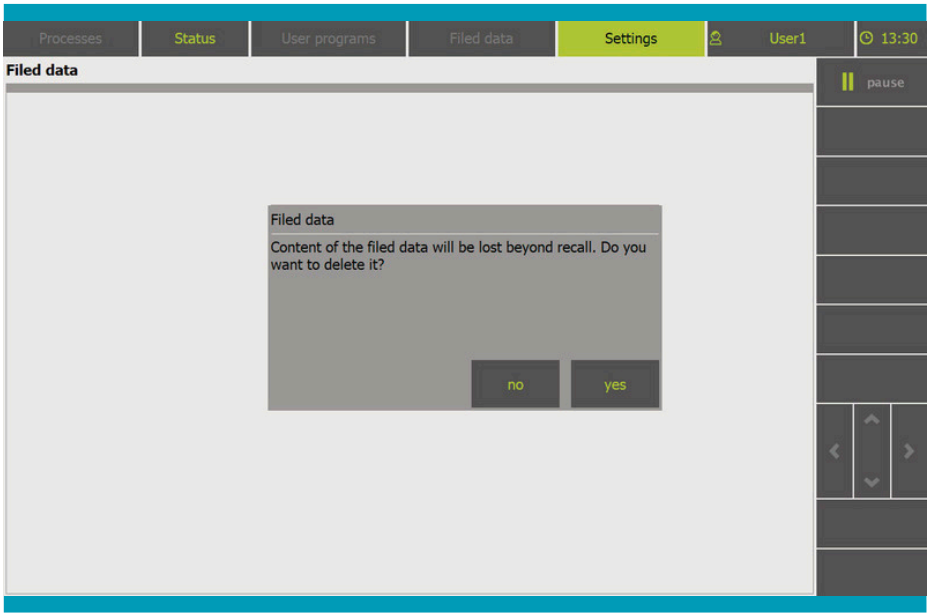
Eliminazione dati

1. Verificare che i file siano stati scaricati completamente.
2. Selezionare <Settings> ▸ <Tools> ▸ <Backup Filed Data> e toccare <run>.
3. Toccare <Delete> (vedere Schermata 8.6).



Schermata 8.6: Selezionare delete

4. Per confermare, toccare <yes> (vedere Schermata 8.7).

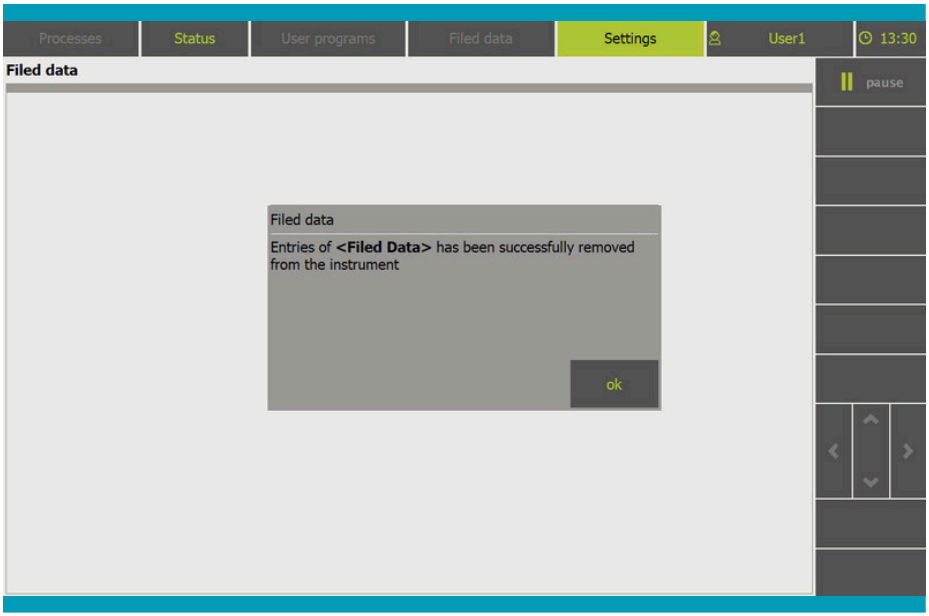


Schermata 8.7: Confermare l'eliminazione dei dati

5. Attendere che il processo di eliminazione sia concluso, quindi toccare <ok> nella finestra di dialogo (vedere Schermata 8.8).
6. Dopo l'eliminazione, tutti i dati in <Filed data> verranno eliminati. Verrà creato un protocollo per l'esecuzione dell'operazione Backup Filed Data.

IMPORTANTE

I dati eliminati non possono essere recuperati.



Schermata 8.8: Eliminazione completata

8.2.3 Chamber In

Questo strumento si usa per inserire la chamber nell'unità CentriCult al di fuori di un'applicazione in esecuzione. L'adattatore di blocco della camera si sposta in posizione di inserimento e sblocca il coperchio di protezione dell'unità CentriCult. Dopo aver eseguito questa operazione, aprire manualmente l'unità CentriCult.

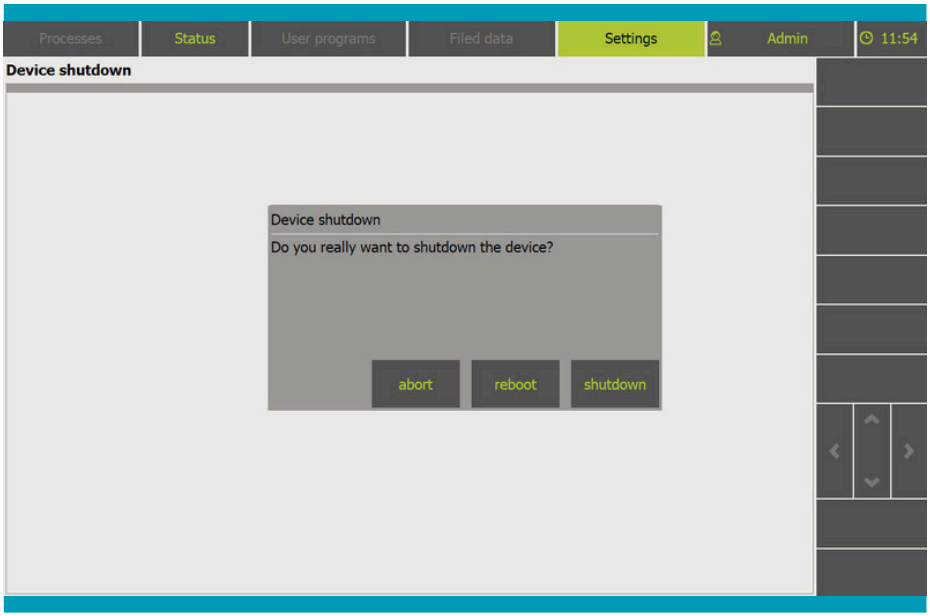
8.2.4 Chamber Out

Questo strumento si usa per rimuovere la chamber dall'unità CentriCult al di fuori di un'applicazione in esecuzione. L'adattatore di blocco della camera si sposta in posizione di sostituzione e sblocca il coperchio di protezione dell'unità CentriCult. Dopo aver eseguito questa operazione, aprire manualmente l'unità CentriCult.

8.2.5 Shutdown (Spegnimento)

Questo comando spegne o riavvia lo strumento.

1. Toccare **<run>** nella barra degli strumenti per eseguire la funzione di spegnimento.
2. Selezionare abort, shutdown o reboot (vedere Schermata 8.9).



Schermata 8.9: Selezionare shutdown o reboot

8.2.6 Recovery (Recupero)

Questo programma consente di salvare i prodotti cellulari in sacche dedicate in caso di interruzione del processo. Questo strumento supporta solo i seguenti set di tubi CliniMACS Prodigy: TS 310, TS 500 e TS 510.

IMPORTANTE
Utilizzare questo strumento solo secondo le indicazioni di Miltenyi Biotec Technical Support.

8.2.7 Strumento Gas Mix (miscela dei gas)

Questo programma consente il campionamento di gas con una sacca di campionamento dall'unità di miscelamento del gas.

8.2.8 Instrument Check (Controllo strumento)

Questo programma esegue un controllo semi-automatico dello strumento e richiede un certo grado di interazione da parte dell'utilizzatore.

8.2.9 Column Load (Caricamento colonna)

In alcuni casi specifici, il processo consente l'arricchimento delle cellule CD34 positive dai prodotti di leucaferesi.

8.2.10 Custom Files (File personalizzati)

Questo programma viene utilizzato per aggiungere CAP allo strumento.

8.2.11 Sealer (Saldatore)

Questo programma viene utilizzato per attivare/disattivare Sealer.

8.3 User settings (impostazioni utente)

Le impostazioni si trovano in **<Settings>** ▸ **<User settings>**.

8.3.1 Set time (Imposta ora)

Questa funzione consente di impostare la data e l'ora sullo strumento.

Nota: l'ora qui impostata viene automaticamente sovrascritta se la sincronizzazione dell'ora di rete è abilitata. Per impostare la sincronizzazione dell'ora di rete, vedere sezione 9.6 ´Abilitazione della sincronizzazione dell'ora di rete´.

8.3.2 Network Settings (Impostazioni di rete)

Questa impostazione contiene le informazioni necessarie per l'integrazione della rete. Per una spiegazione dettagliata, consultare le sezioni seguenti:

- 9.1 per l'integrazione della rete
- 9.2 per la connessione LDAP
- 9.3 per la condivisione di file
- 9.4 per il trasferimento di file tramite FTP
- 9.6 per la sincronizzazione dell'ora della rete

Per impostare la notifica via e-mail vedere sezione 9.5 ´Connessione a un server di posta elettronica´

8.3.3 Custom settings (Impostazioni personalizzate)

Custom settings comprende impostazioni generali per lo strumento, tra cui la lingua, il nome dell'azienda, il dipartimento, la via, il codice di avviamento postale, la città, il nome dello strumento, la persona di contatto, la località.

L'impostazione della notifica via e-mail si trova anche in Customer settings, vedere sezione 9.5 ´Connessione a un server di posta elettronica´.

8.3.4 Module settings (Impostazioni modulo)

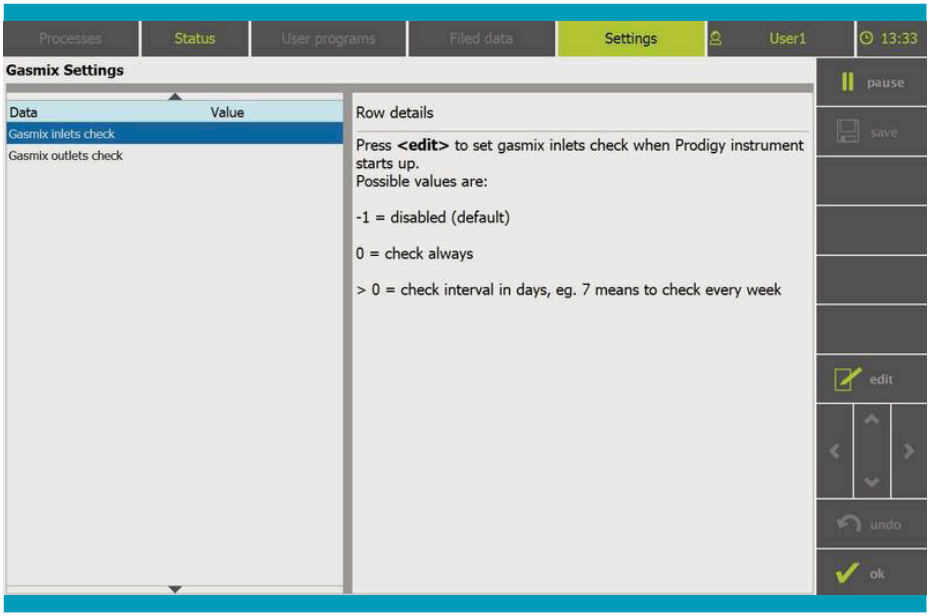
Module settings comprende le configurazioni per il test dell'hardware, tra cui:

- Controllo ingressi della miscela di gas
- Controllo uscite della miscela di gas
- Controllo della rotazione
- Promemoria Supplementary Bag

Per ciascuno di questi componenti, è possibile impostare l'esecuzione dei controlli a intervalli di tempo diversi:

- Mai (-1)
- Sempre (0)
- Periodicamente (inserire il numero in giorni).

Per una configurazione esemplificativa degli ingressi della miscela dei gas vedere Schermata 8.10.



Schermata 8.10: Controllo ingressi della miscela di gas

8.3.5 Settings exchange tool (Strumento di scambio impostazioni)

Il comando <Settings Exchange> consente di copiare le configurazioni in più strumenti. Queste impostazioni includono:

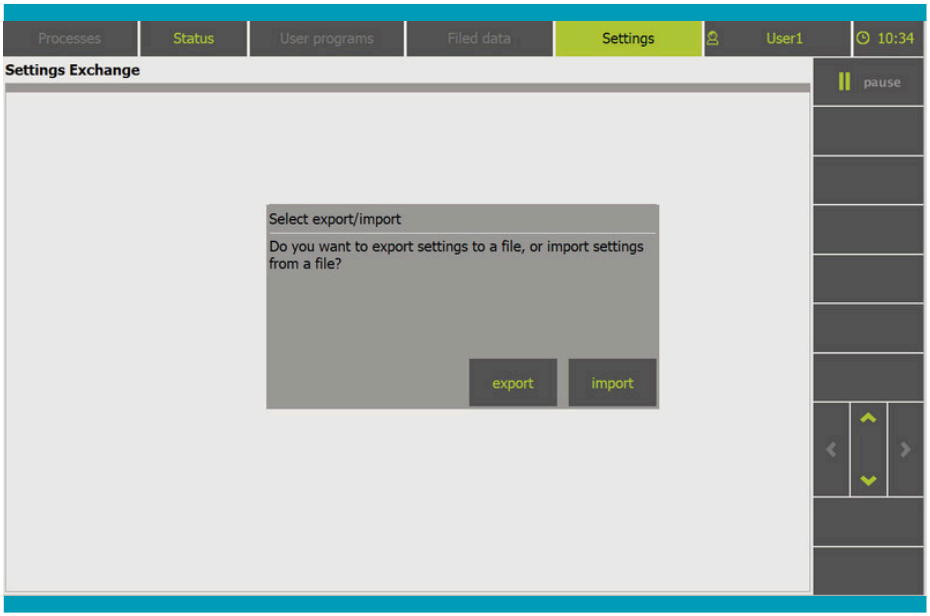
- Customer settings (Impostazioni personalizzate)
- Gasmix settings (Impostazioni della miscela di gas)
- Module settings (Impostazioni modulo)
- Network Settings (Impostazioni di rete)

IMPORTANTE

- Se si utilizza una penna USB per l'importazione o l'esportazione, questa deve essere in formato FAT32 e non deve essere protetta da password.
- Se la condivisione dei file è configurata, i file possono essere esportati anche nella cartella di condivisione dei file (vedere sezione 9.3 ´Connessione a un drive di rete´).

Esportazione di impostazioni su penna USB

1. Inserire una penna USB.
2. Selezionare <Settings> ▸ <User settings> ▸ <Setting Exchange> e toccare <run >.
3. Toccare <export> nella finestra di dialogo (vedere Schermata 8.11).



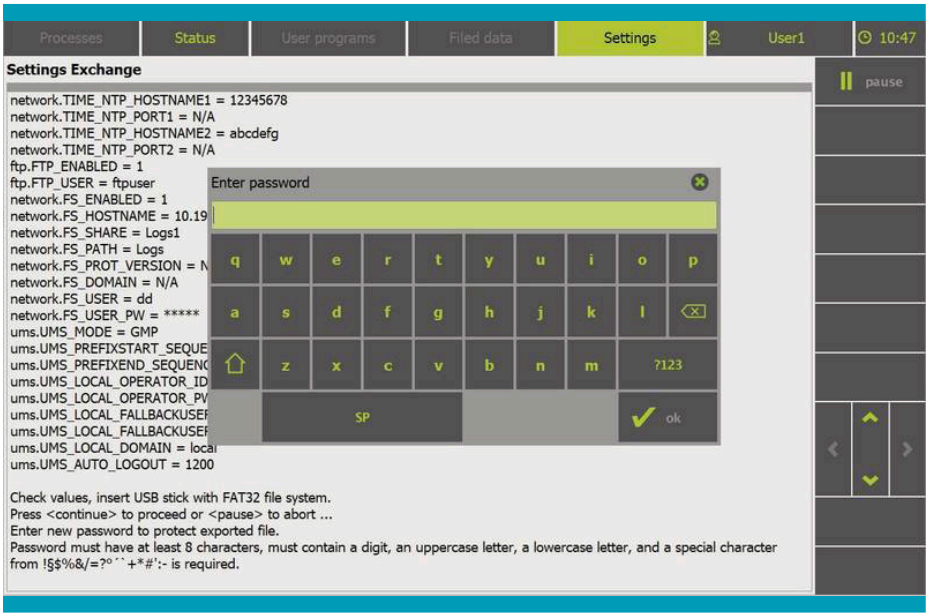
Schermata 8.11: Selezionare export

4. Controllare i valori sullo schermo. Toccare <continue> nella barra degli strumenti.



Schermata 8.12: Controllare i valori delle impostazioni

5. Inserire la password per il login.



Schermata 8.13: Inserire la password

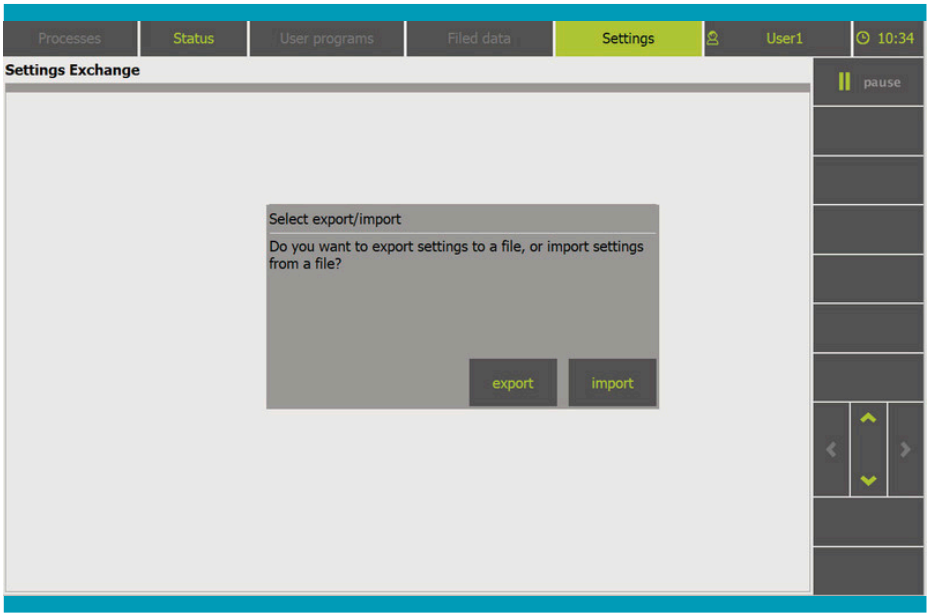
Importazione delle impostazioni da una penna USB

1. Inserire una penna USB con il file delle impostazioni utente desiderate.

   Nota: la penna USB deve essere in formato FAT32 e non deve essere protetta da password.

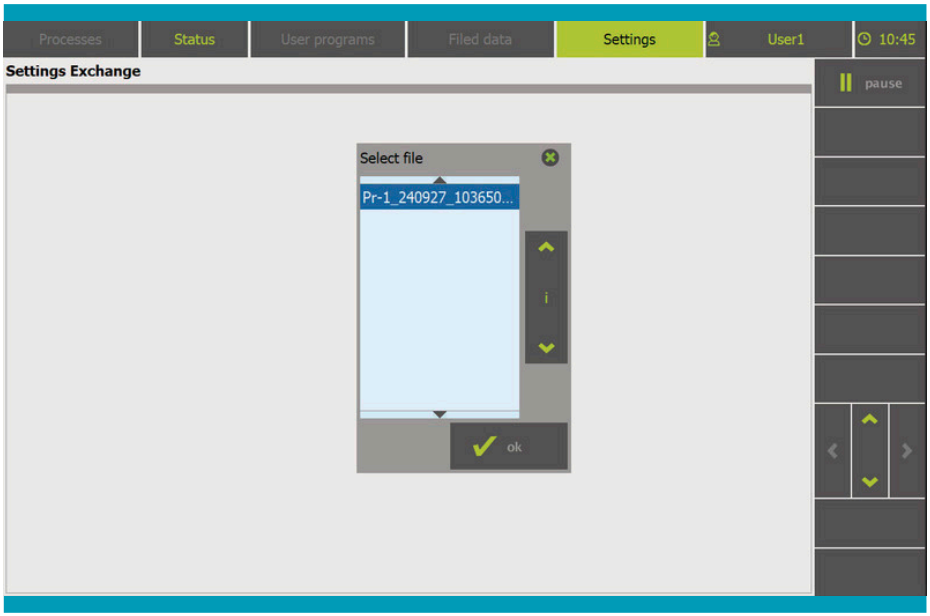
2. Selezionare **<Settings>** ▸ **<User settings >** ▸ **<Setting Exchange>** e toccare **<run>**.

3. Selezionare **<Import>** nella finestra di dialogo (vedere Schermata 8.14).



Schermata 8.14: Selezionare import

4. Selezionare i file da importare e toccare <ok> (vedere Schermata 8.15).



Schermata 8.15: Selezionare il file da importare

5. Inserire la password per il login (vedere Schermata 8.13).

8.3.6 Set Volume (Imposta volume)

Questo programma imposta il volume dell'altoparlante dello strumento.

8.3.7 N_2 Settings (Impostazioni N_2)

Questo programma configura le due porte dei gas dello strumento da utilizzare tra le tre disponibili (N_2, CO_2 aria compressa).

9 Integrazione di rete

È possibile connettere lo strumento alla rete locale tramite un adattatore da USB a Ethernet. Per utilizzare le seguenti funzioni è necessaria un'adeguata integrazione di rete:

- User Management centralizzato (LDAP)
- Trasferimento di file tramite FTP
- Condivisione automatica di file
- Notifica via mail
- Sincronizzazione dell'ora di rete

Per utilizzare le funzioni precedenti, connettere prima lo strumento alla rete locale consultando la sezione 9.1 ´Connessione a una rete locale´, quindi seguire le istruzioni per le funzioni specifiche.

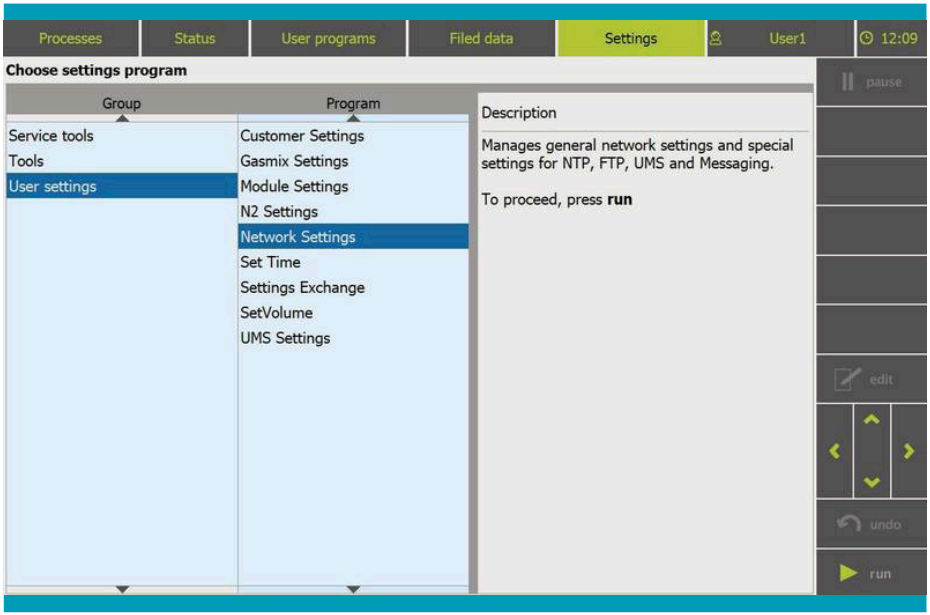
IMPORTANTE

- Solo gli utenti UMS con ruolo di amministratore 'Administration tools user' o gli utenti con diritti 'Network Setting' hanno accesso a questa impostazione. Per configurare diritti e ruoli, vedere il capitolo 10 'Gestione degli utenti'.
- Il pulsante **<Connectivity Hub>** può essere visualizzato sullo schermo ma è correntemente disabilitato e resterà disabilitato finché questa funzione non sarà supportata.
- L'utente deve assicurarsi che le impostazioni del firewall consentano lo scambio di dati tra lo strumento e il server/client desiderato. Il cliente è responsabile della configurazione delle impostazioni del firewall.
- Alcune modifiche alle impostazioni richiedono il riavvio dello strumento per essere applicate.

9.1 Connessione a una rete locale

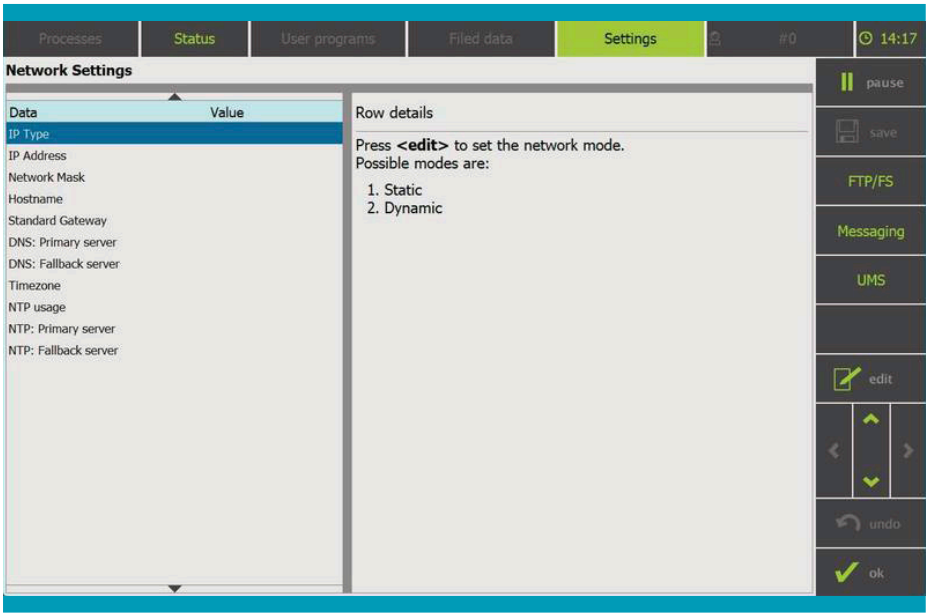
1. Connettere lo strumento alla rete locale utilizzando un adattatore da USB a Ethernet.

2. Per accedere alle impostazioni di rete, selezionare <Settings> ▸ <User settings> ▸ <Network Settings> e toccare <run> (vedere Schermata 9.1). Verrà visualizzato Network Settings (Schermata 9.2).



Schermata 9.1: Selezionare Network Settings

3. Per scegliere tra indirizzo IP statico e indirizzo IP dinamico, selezionare <IP Type> dall'elenco e toccare <edit> nella barra degli strumenti, quindi inserire il valore desiderato nel campo di inserimento.



Schermata 9.2: Network Settings (Impostazioni di rete)

Per gli indirizzi IP statici, procedere come segue:

1. Selezionare <IP Address> nell'elenco e toccare <edit> nella barra degli strumenti, quindi inserire l'indirizzo IP nel campo di inserimento.
2. Selezionare <Network Mask> nell'elenco e toccare<edit>, quindi inserire la maschera di rete nel campo di inserimento.
3. Per inserire il nome dello strumento, selezionare <Hostname> e toccare <edit>.
4. Per inserire l'indirizzo IP del gateway, selezionare <Standard Gateway> e toccare <edit>.
5. Opzionale: Per scegliere il fuso orario, selezionare <Timezone> e toccare <edit>. Il fuso orario predefinito dello strumento è il tempo coordinato universale (UTC).
6. Verificare che lo strumento sia connesso alla rete locale.

Per gli indirizzi IP dinamici, procedere come segue:

1. Per inserire il nome dello strumento, selezionare <Hostname> e toccare <edit>.
2. Il server dinamico deve essere configurato. Inserire un indirizzo IP per il server primario (primary) e quello di riserva (fallback).
3. Opzionale: Per scegliere il fuso orario, selezionare <Timezone> e toccare

<edit>. Il fuso orario predefinito dello strumento è il tempo coordinato universale (UTC).

4. Verificare che lo strumento sia connesso alla rete locale.

IMPORTANTE
Se nella propria organizzazione le porte di rete sono protette da filtri per gli indirizzi MAC, contattare il proprio fornitore di servizi IT locale per la configurazione corretta.

9.2 Connessione a un server LDAP

Per configurare la connessione al server LDAP, selezionare (menu di accesso rapido) e selezionare <User Management>. Nel menu <User Management> selezionare <Configuration> ▸ <LDAP Configuration>. Per configurare LDAP, procedere come segue (vedere Figura 9.1).

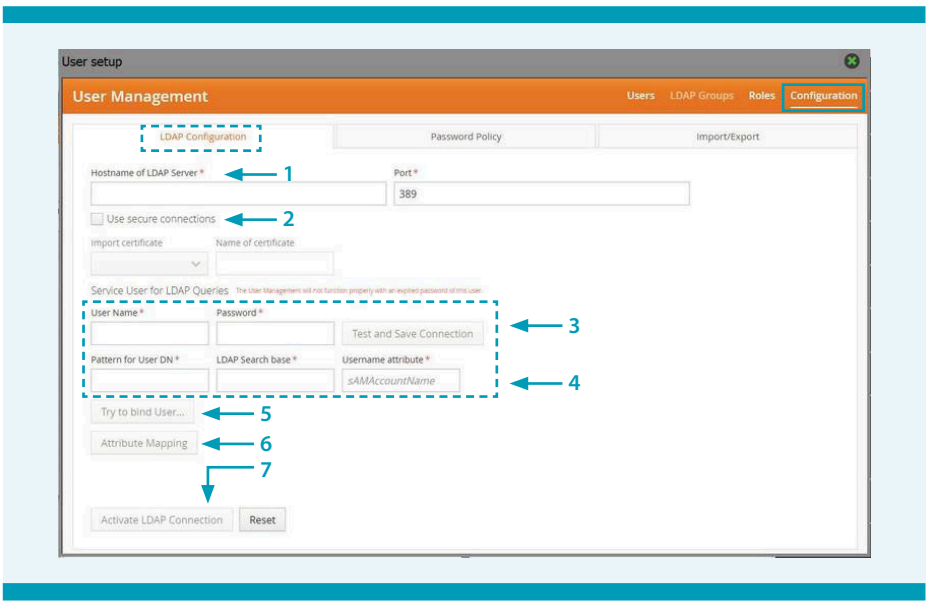


Figura 9.1: Menu User Management e passaggi necessari per configurare LDAP

1. Inserire il nome host/indirizzo IP del server LDAP.
2. Selezionare una connessione sicura se richiesto. Per una connessione LDAP sicura, sarà impostata automaticamente la porta 636 al posto della porta standard 389. Per una connessione sicura, seguire le istruzioni riportate nella sezione 10.4.2 ´Importazione impostazioni in UMS´ per importare il certificato in Prodigy Instrument e selezionare il certificato nell'elenco <import certificate>.
3. Inserire il nome utente e la password di un account LDAP valido. È necessario

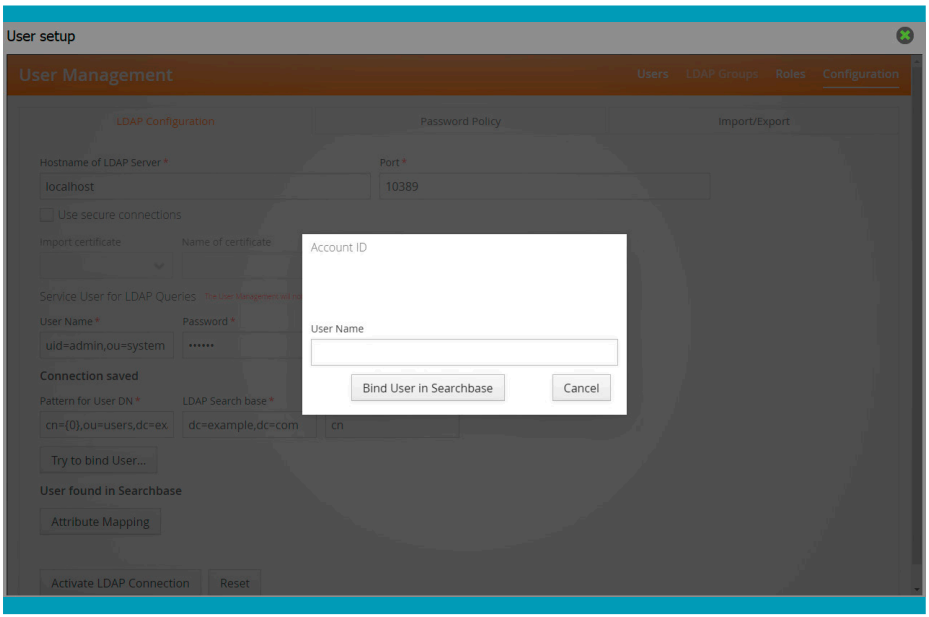
inserire il percorso LDAP completo del nome utente. Toccare <Test and Save Connection>. Verrà visualizzato un pop-up per indicare che la connessione è avvenuta con successo.

4. Inserire il modello, la base di ricerca e l'attributo del nome utente. Il modello per il nome del dominio utente deve contenere il percorso completo. Questi inserimenti dipendono dalla struttura organizzativa LDAP dell'utente e dal nome del dominio. Per visualizzare una breve spiegazione ed esempi di valori tipici, passare il mouse sopra le caselle di testo. Potrebbe essere utile disporre di un accesso a un programma browser basato su LDAP per visualizzare le unità organizzative nel browser.

   I valori tipici sono indicativamente:

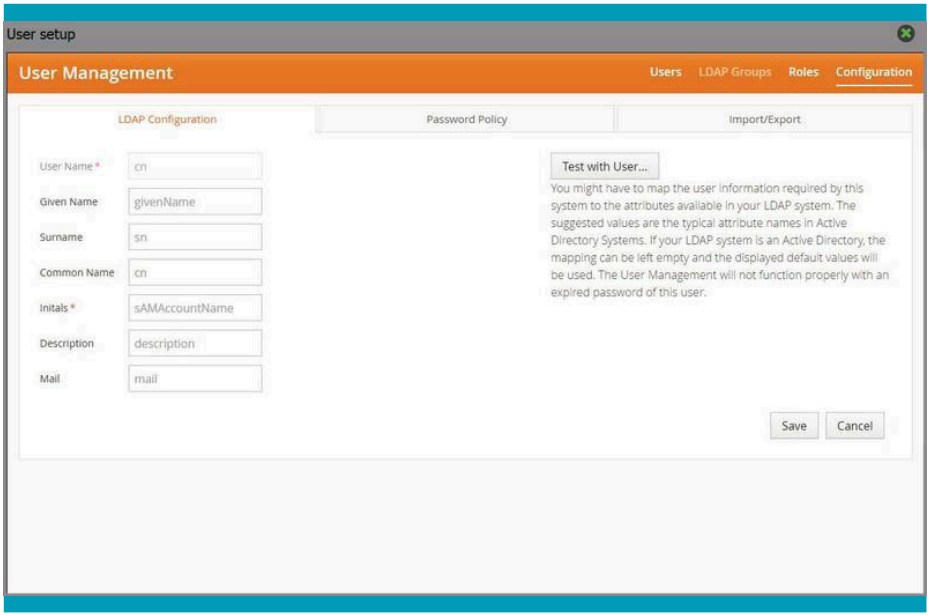
   - Modello = '<domain>/{0}', ad esempio 'customername_dev/{0}'
   - Base di ricerca = 'OU=organization,DC=customername'
   - Attributo del nome utente = 'sAMAccountName'

5. Toccare <Try to bind User....>. Verrà visualizzato un pop-up (Schermata 9.3). Inserire un nome utente valido (il nome utente può essere lo stesso utilizzato per il test di login). Quindi toccare <Bind User in Searchbase> per continuare. Se l'operazione va a buon fine, la finestra pop-up Account ID viene chiusa; in caso contrario, verrà visualizzato un messaggio di errore.



Schermata 9.3: Pop-up di inserimento di Account ID per inserire un nome utente valido

6. Toccare <Attribute Mapping>. Verrà visualizzata la mappatura degli attributi (Schermata 9.4). L'attributo nome utente inserito al passaggio 4 verrà automaticamente mappato al nome utente. In 'initials', inserire lo stesso valore di 'User Name'. Inserendo qui i valori, al momento della creazione dell'utente alcune informazioni vengono immesse automaticamente. Toccare <save> per tornare alla pagina della configurazione LDAP.
7. Toccare <Activate LDAP Connection>. Questo pulsante è attivo se i passaggi 3, 4 e 5 sono andati a buon fine.



Schermata 9.4: Esempio di attributi precompilati

IMPORTANTE

È necessario impostare un valore per 'initials' (vedere Schermata 9.4) poiché questo valore è considerato un'informazione obbligatoria per gli utilizzatori di CliniMACS Prodigy. La mancata o errata configurazione della mappa degli attributi può causare un errore di login.

Seguendo questi sette passaggi (vedere Figura 9.1), è possibile configurare interamente la connessione LDAP e quindi usarla per creare gruppi LDAP e utenti LDAP in <User Management>. Ulteriori dettagli sulla gestione degli account e dei ruoli sono riportati nel capitolo 10 ´Gestione degli utenti´.

9.3 Connessione a un drive di rete

La condivisione automatica dei file trasferisce tutti i logfile sull'unità di rete subito dopo che l'applicazione ha completato l'esecuzione del processo. I record audit trail possono essere esportati nell'unità di rete anche manualmente dall'utente (vedere sezione 7.2.2 ´Esportazione di audit trail´). Il trasferimento automatico dei file è implementato sulla base del protocollo Server Message Block (SMB). Le versioni supportate del protocollo SMB sono SMB 1.0, SMB 2.1 e SMB 3.0 (predefinita).

Nota: si consiglia di utilizzare SMB 2.0 e SMB 3.0. SMB 1.0 è supportato solo per motivi di legacy e deve essere utilizzato solo per interagire con dispositivi obsoleti in caso di estrema necessità..

Prerequisiti

- Server SMB: assicurarsi che il server SMB sia raggiungibile. Controllare la versione del protocollo SMB di questo server prima di iniziare.
- Una cartella precedentemente creata sul server SMB per l'archiviazione dei dati. Annotare il nome della condivisione. Può trattarsi di condivisione anonima (accessibile all'account ospite) o autenticata (accessibile solo all'account specificato).

  Nota: si consiglia la condivisione autenticata per garantire la sicurezza dei dati.

- Se si usa la condivisione autenticata, è necessario un account protetto da password, il quale deve avere diritti di lettura e scrittura alla cartella di condivisione sul server SMB.
- Lo strumento è connesso a Ethernet e la rete è abilitata.

Configurazione dello strumento

Nota: è importante inserire tutti i parametri di condivisione dei file prima di abilitare l'opzione di condivisione file, poiché qualsiasi modifica successiva disabiliterà la condivisione dei file. Una volta configurate le impostazioni, lo strumento deve essere riavviato per completare la configurazione. Le modifiche alla configurazione del trasferimento dei file vengono applicate durante il riavvio.

1. Per aprire FTP/File Share settings, toccare **<FTP/FS>** nella barra degli strumenti (Schermata 9.2).
2. In **<FTP/File Share Settings>**, solo i parametri nel riquadro blu sono rilevanti per la condivisione di file (vedere Figura 9.2).

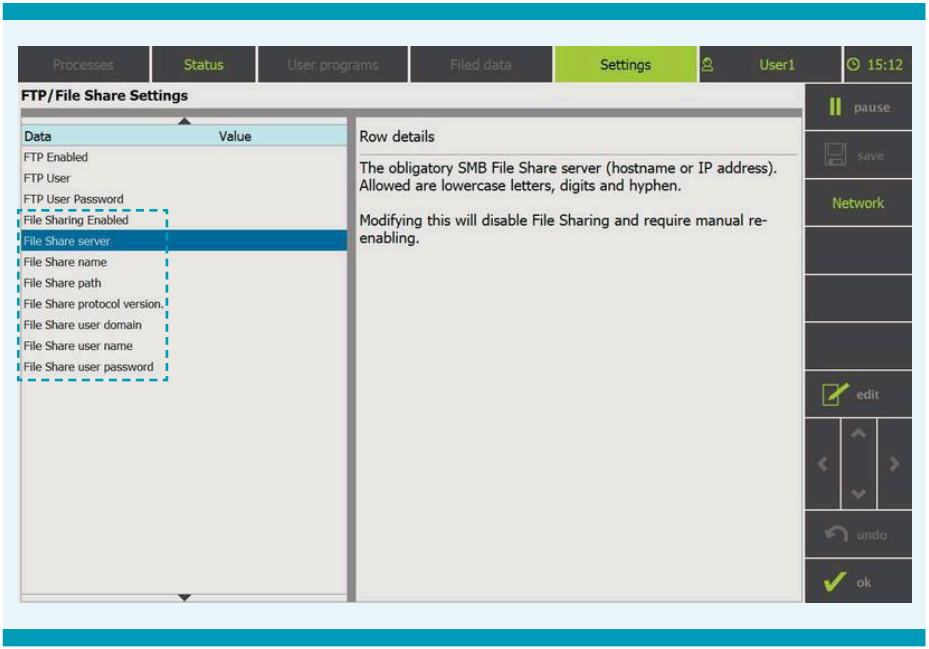


Figura 9.2: Parametri per la condivisione di file

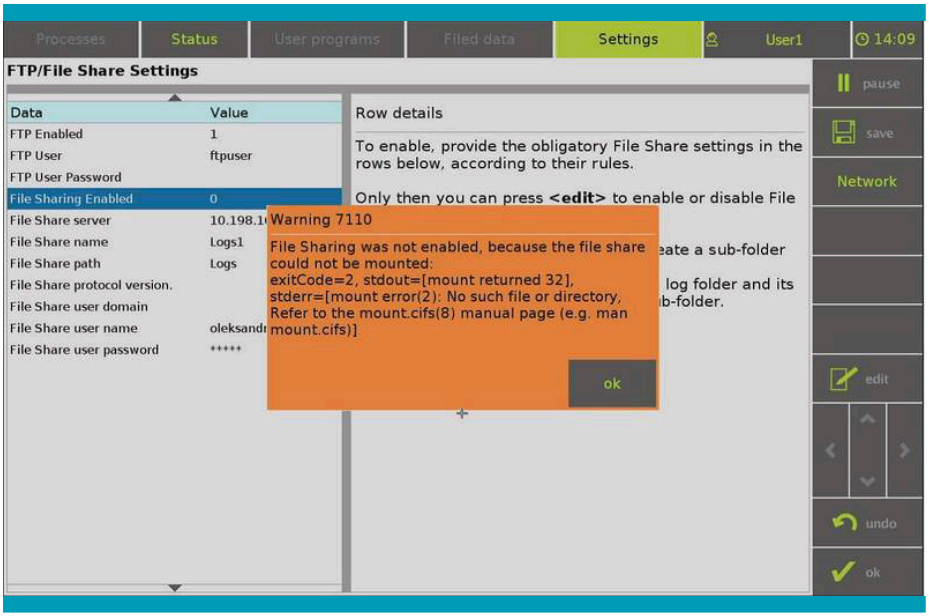
2. Per inserire il nome host o l'indirizzo IP del server SMB, selezionare **<File Share server>** e toccare **<edit>**.

3. Per inserire il nome condivisione, selezionare **<File Share name>** e toccare **<edit>**.

4. (Opzionale) Selezionare **<File Share path>** e toccare **<edit>** per inserire il percorso.
   Inserendo questo percorso, i file generati dagli strumenti vengono inviati a \\[File Share server]\[File Share name]\[File Share path]\

   Se questo percorso è vuoto, i file generati vengono inviati a \\[File Share server]\[File Share name]\ Se la cartella non viene trovata, il software genererà un avviso (Schermata 9.5).

IMPORTANTE
Si raccomanda di non utilizzare spazi nel percorso File Share.



Schermata 9.5: Avviso di errore di configurazione della condivisione di file

5. Per inserire la versione del protocollo SMB selezionare <File Share protocol version> e toccare <edit>.

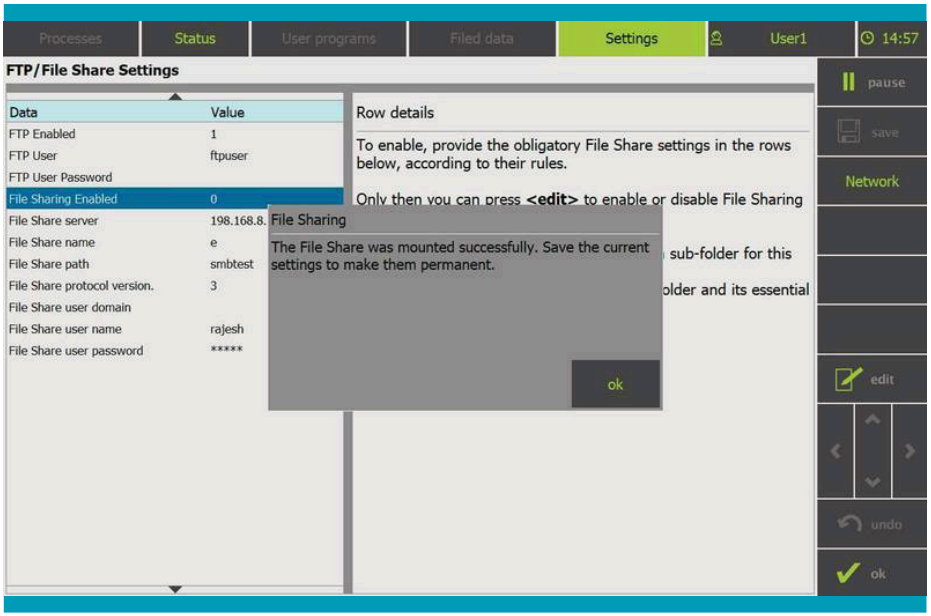
6. Per inserire il dominio utente selezionare <File Share user domain> e toccare <edit>. Ripetere i passaggi per <File Share user name> e <File Share user password>.

IMPORTANTE

Se si usa 'Guest' come utente per la condivisione della cartella di archiviazione, il dominio utente File Share, il nome utente File Share e la password utente File Share devono essere vuoti.

7. Impostare <File Sharing Enabled> su 1.

Dopo la configurazione, un pop-up informa sulla riuscita della configurazione (vedere Schermata 9.6).



Schermata 9.6: Configurazione riuscita per la condivisione di file

IMPORTANTE

Modificandone i parametri, la condivisione di file viene disabilitata e deve essere riabilitata manualmente. Controllare sempre che 'File Sharing Enabled" sia abilitato (valore impostato su 1).

9.4 Configurazione del trasferimento di file tramite FTP

FTP è un protocollo di rete che consente il trasferimento di dati tra CliniMACS Prodigy (definito server FTP) e il computer dell'utente finale (definito client FTP) attraverso connessioni IP (Internet Protocol).

IMPORTANTE

- Assicurarsi che la connessione FTP sia utilizzata solo in una rete interna, isolata in entrambe le direzioni da Internet. La sicurezza della rete deve essere garantita dall'utente.
- Assicurarsi che le impostazioni del firewall sul computer client siano configurate in modo corretto per le connessioni FTP attive o passive al fine di consentire lo scambio di dati con lo strumento.

Nota: i dati accessibili da CliniMACS Prodigy tramite FTP sono in sola lettura e possono solo essere scaricati

Per connettere il client FTP allo strumento, è necessario effettuare il login. Lo

strumento deve essere configurato in modo diverso a seconda dell'opzione di login. Sono supportate due opzioni di login:

- Opzione di login 1: un account registrato in UMS. Assicurarsi che il ruolo 'File management user' sia assegnato a questo account. In questo caso, l'avvio e la chiusura della connessione saranno registrate nell'audit trail. Per ulteriori informazioni su ruoli e gestione degli utenti, consultare il capitolo 10 ´Gestione degli utenti´.
- Opzione di login 2: un nome utente e una password locali salvati in FTP/File Share Settings.

9.4.1 Configurazione dello strumento

1. Selezionare <FTP/File Share Settings>. Solo i parametri nel riquadro blu sono rilevanti per l'FTP.

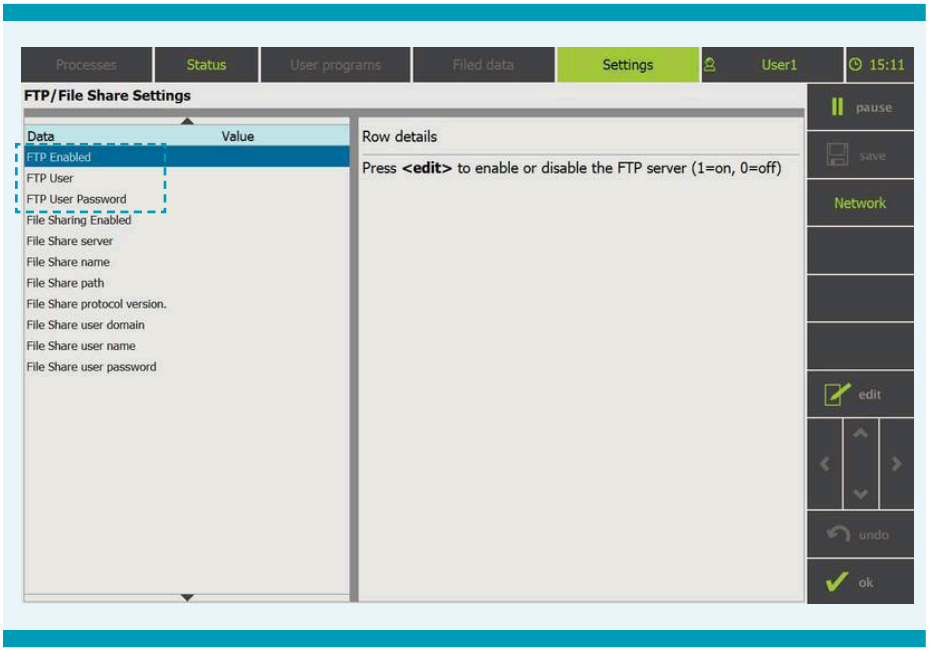


Figura 9.3: Parametri per la condivisione di file

2 (Saltare questo passaggio, per l'opzione di login 1) Per inserire il nome utente quando si effettua il login dal client FTP, selezionare <FTP User> e toccare <edit>. Il nome utente utilizzato per il client FTP non necessita di essere registrato nel sistema di gestione degli utenti. Il nome utente deve iniziare con una lettera e può contenere maiuscole e minuscole, numeri e trattini bassi.

Nota: se <FTP User> è impostato su 'N/A', la connessione FTP è disabilitata.

3. (Saltare questo passaggio per l'opzione di accesso 1) Per inserire la password, selezionare < FTP User Password > e toccare < edit >. La password deve contenere almeno sei caratteri e può essere composta da maiuscole e minuscole, numeri e caratteri speciali,.:+#!?=.
4. Per abilitare la connessione FTP, selezionare <FTP Enabled> e impostare il valore su 1 nel campo di inserimento.
5. Per salvare le impostazioni, toccare <ok> nella barra degli strumenti.

9.4.2 Connessione con client FTP

Completata la configurazione, l'utente può effettuare la connessione allo strumento con qualsiasi client FTP disponibile (ad es. FileZilla) per scaricare protocolli e logfile. Per la connessione allo strumento, inserire le seguenti informazioni:

- L'indirizzo IP dello strumento, si trova in <Settings> ▸ <Tools> ▸ <Info> ▸ <Network information>.
- Ingresso: usare la porta standard 21.
- Nome utente e password: Per l'opzione di login 1: inserire l'ID account e la password registrati in User Management.
  Per l'opzione di login 2: inserire il nome utente e la password impostati come descritto in precedenza nei passaggi 2 e 3.

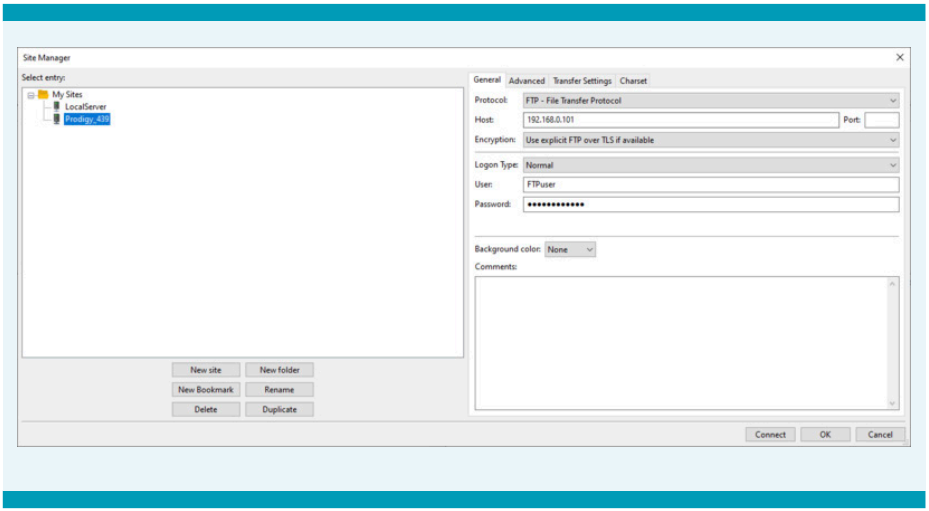


Figura 9.4: Parametri di connessione esemplificativi

Nota: un singolo utente può stabilire una sola connessione alla volta, poiché il server dello strumento non consente connessioni multiple. Con software client che utilizza connessioni simultanee (ad es. FileZilla), occorre modificare di conseguenza

le impostazioni del client per consentire una singola sessione. In caso contrario, sarà possibile consultare i contenuti ma non scaricarli.

9.5 Connessione a un server di posta elettronica

In caso di messaggi di errore e/o di avvisi durante l'esecuzione di un processo, il software può inviare un'e-mail a un indirizzo di posta elettronica precedentemente inserito. L'e-mail conterrà avvisi/messaggi di errore e uno screenshot dello strumento (vedere Figura 9.5). La notifica via e-mail supporta il Simple Mail Transfer Protocol (SMTP) e il Simple Mail Transfer Protocol Secure (SMTPS).

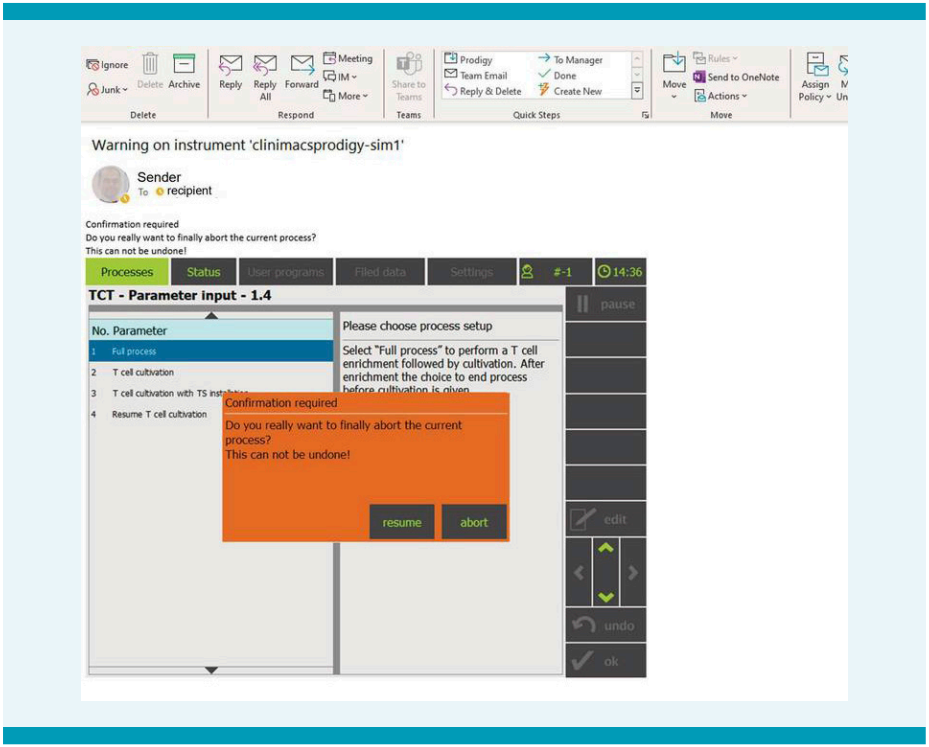


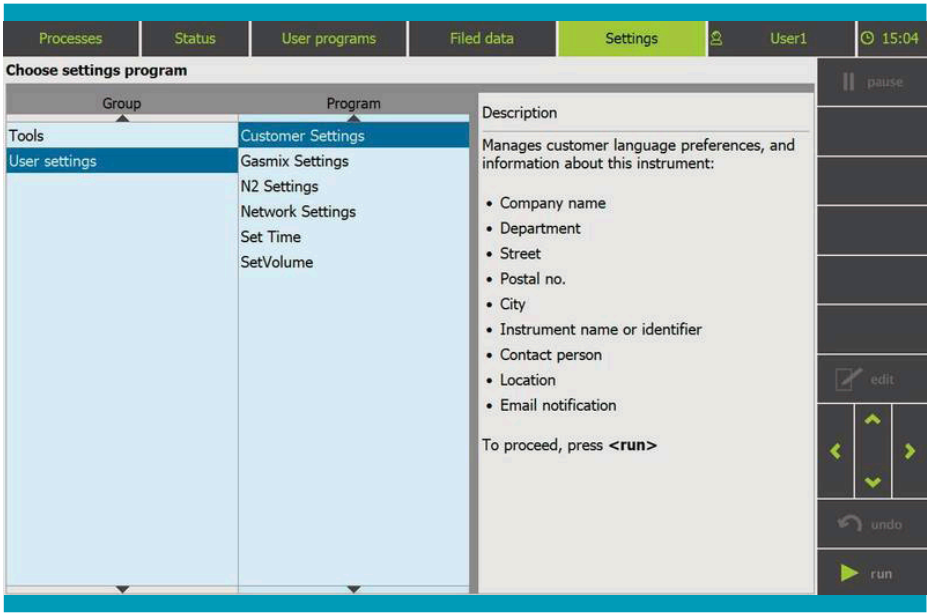
Figura 9.5: Esempio di e-mail

Prerequisiti:

- Un server di posta elettronica che supporta il protocollo SMTP o SMTPS. Assicurarsi che il server sia raggiungibile. Annotare l'indirizzo IP e l'ingresso del server.
- Un account di posta elettronica del cliente creato precedentemente, che può essere utilizzato per l'autenticazione durante la configurazione
- Lo strumento è connesso alla rete Ethernet e la rete è abilitata.

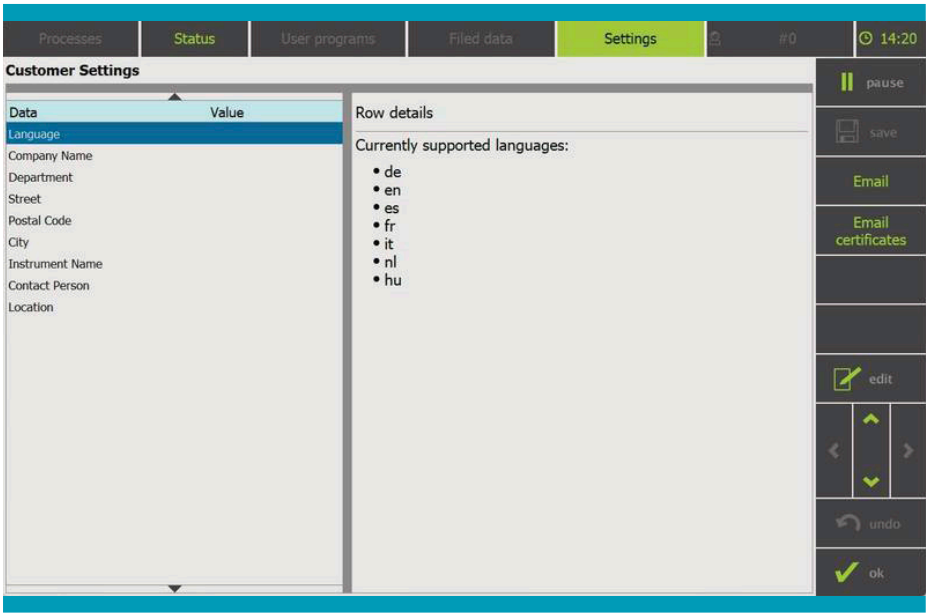
Configurazione dello strumento:

1. Per inserire le impostazioni personalizzate, selezionare <Settings> ▸ <User settings> ▸ <Customer Settings> e toccare <run> (vedere Schermata 9.7).



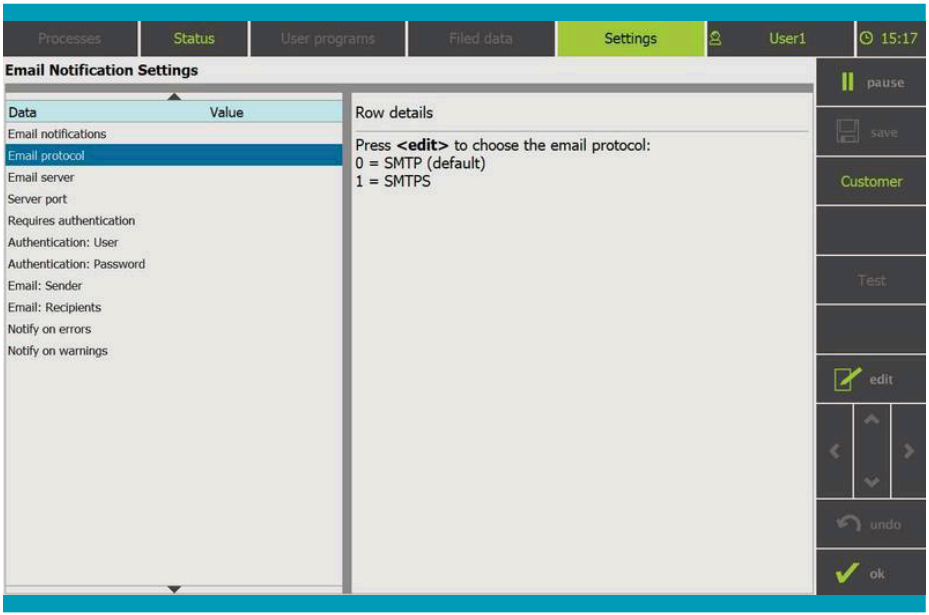
Schermata 9.7: Avviare le impostazioni personalizzate

2. Per inserire <Email Notification Settings> toccare <Email> nella barra degli strumenti (vedere Schermata 9.8).



Schermata 9.8: Impostazioni e-mail

3. Per inserire il valore corrispondente al protocollo usato dal server e-mail, selezionare <Email protocol> e toccare <edit>. Di default, è selezionato SMTP(0).



Schermata 9.9: Parametri per la notifica via e-mail

4. Per inserire il nome host o l'indirizzo IP del server di posta elettronica, selezionare <Email server>.

5. Per inserire la porta utilizzata nel server di posta elettronica, selezionare <Server port> e toccare <edit>.

Se si utilizza la porta standard, non è necessario modificare questo campo.

Protocollo	Porta predefinita	Porta alternativa
SMTP	25	2525, 465, 587
SMTPS	465	587 (TLS)

Tabella 9.1: Porta per il server di posta elettronica

6. Selezionare <Requires authentication>. Se il server di posta elettronica richiede l'autenticazione, impostare questo campo su 1 e inserire il nome utente e la password usati per l'autenticazione come descritto al passaggio 7, altrimenti andare al punto 9.

7. Per inserire il nome utente e la password, selezionare <Authentication: User> e <Authentication: Password>. **Nota:** un account di autenticazione può essere condiviso da più strumenti. Se necessario, consultare il proprio dipartimento IT per assistenza.

8. Per inserire l'indirizzo e-mail del mittente, selezionare <Email: Sender> e toccare <edit>. <Email: Sender> può coincidere con l'utente che effettua l'autenticazione.

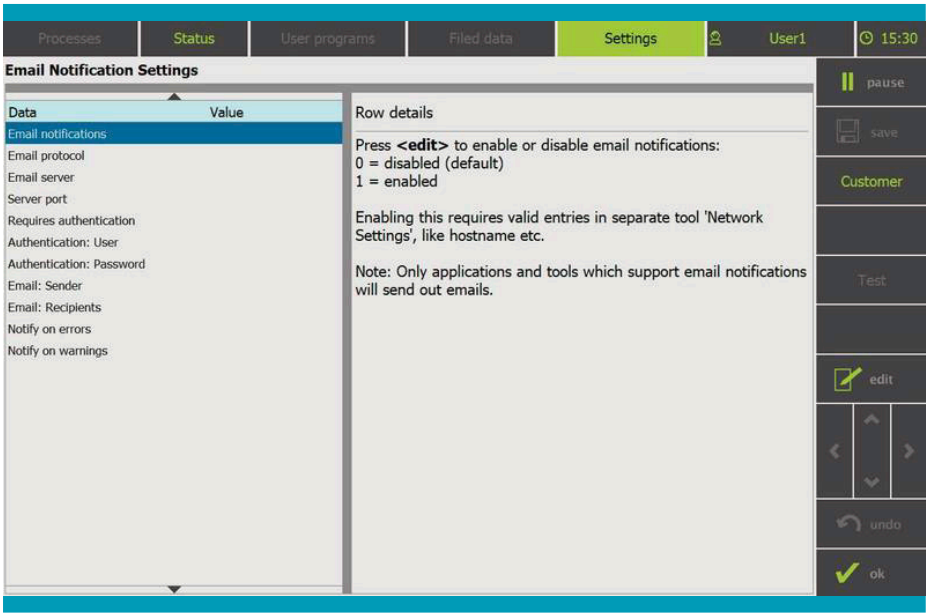
9. Per inserire gli indirizzi e-mail dei destinatari, selezionare <Email: Recipients> e toccare <edit >. Il destinatario può anche essere un indirizzo e-mail di gruppo.

Nota: è possibile inserire più destinatari separandoli con uno spazio.

10. Se si ricevono messaggi di errore, selezionare <Notify on errors> e toccare <edit>. Per abilitare i messaggi, impostare il valore su 1. Di default, la funzione <Notify on errors> è disabilitata (valore impostato su 0).

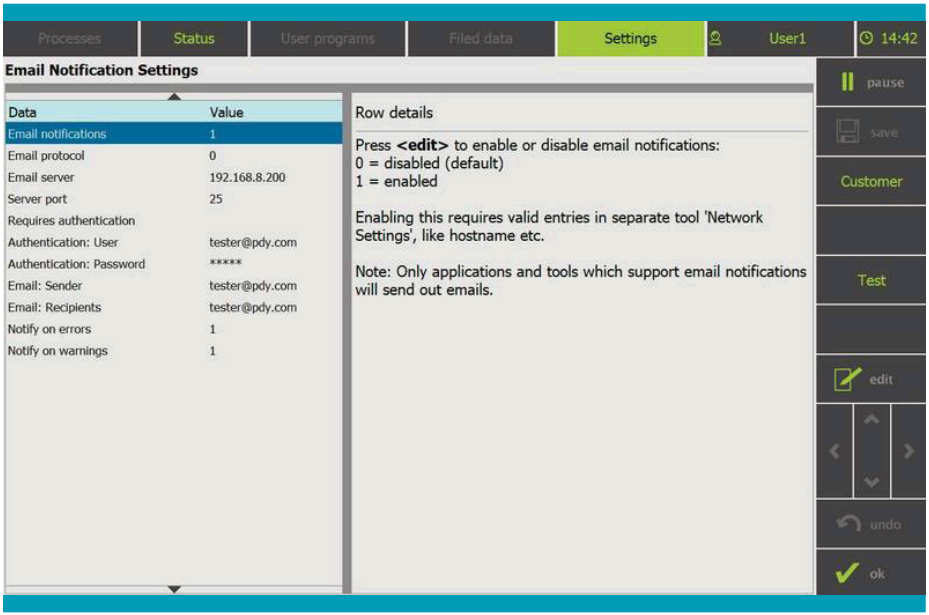
11. Se si ricevono messaggi di avviso, selezionare <Notify on warnings> e toccare <edit>. Per abilitare i messaggi, impostare il valore su 1. Di default, la funzione <Notify on warnings> è disabilitata (valore impostato su 0).

12. Per abilitare le notifiche via e-mail, selezionare < Email notifications > e toccare < edit > (vedere Schermata 9.10). Per abilitare le notifiche, impostare il valore su 1. Di default, le notifiche via e-mail sono disabilitate (valore impostato su 0).



Schermata 9.10: Abilitazione della notifica via e-mail

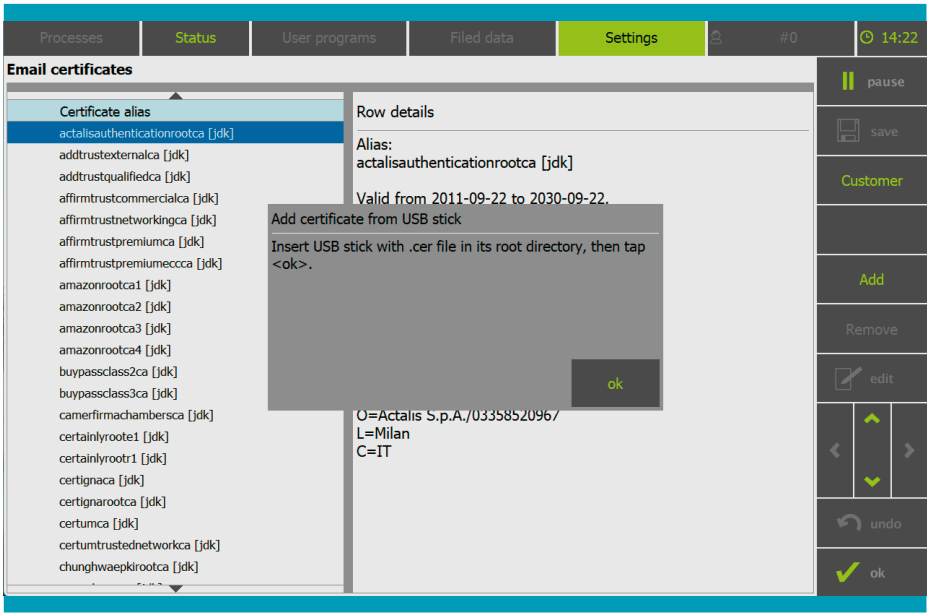
13. Quando tutte le informazioni richieste sono state inserite, viene abilitato il pulsante <Test> sulla barra degli strumenti. Per inviare un'e-mail di prova, toccare <Test> nella barra degli strumenti.



Schermata 9.11: Inviare un'e-mail di prova

Certificati e-mail

Alcuni dei certificati più comuni sono disponibili sul dispositivo. Se sono richiesti ulteriori certificati, questi devono essere caricati.



Schermata 9.12: Aggiungere certificato da chiavetta USB

Per aggiungere un nuovo certificato, premere < Add > e seguire le istruzioni sullo schermo.

9.6 Abilitazione della sincronizzazione dell'ora di rete

NTP è un protocollo di rete che consente la sincronizzazione dell'orologio e la gestione centralizzata dell'ora.

Solo gli utenti UMS con ruolo di amministratore 'Administration tools user' o un utente con ruolo 'network setting tools user' possono accedere alle impostazioni di rete. Per abilitare la funzionalità NTP sullo strumento, procedere come segue:

1. Selezionare <Settings> ▸ <User Settings> ▸ <Network Settings> e toccare <run>. Viene visualizzata la configurazione di rete. I parametri nel riquadro blu sono rilevanti per la sincronizzazione dell'ora di rete (vedere Figura 9.6).

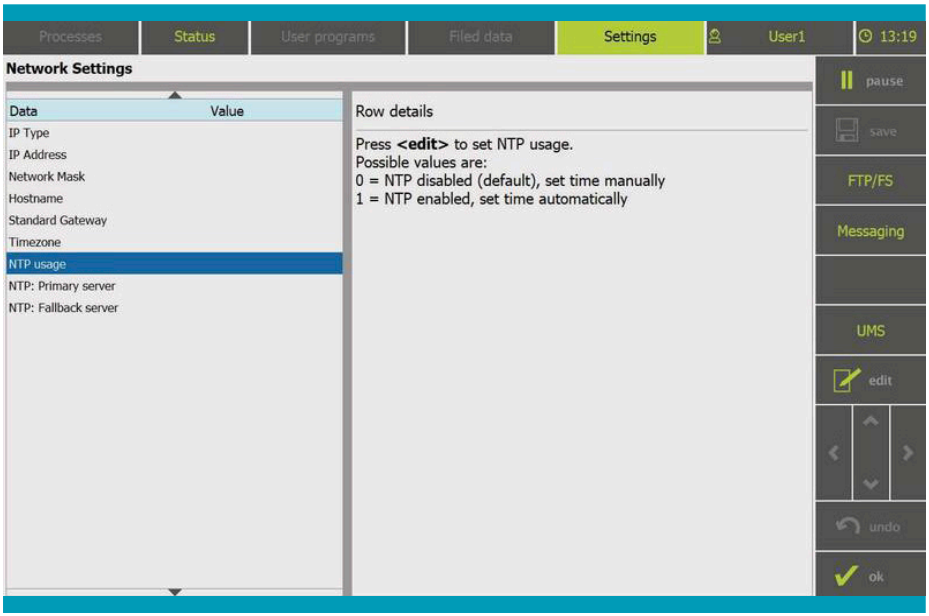


Figura 9.6: Impostazione di NTP

2. Per abilitare NTP e impostare automaticamente l'ora, toccare <NTP usage> e impostare il valore su 1, quindi toccare <ok> nel campo di inserimento.
3. Per inserire il nome host/indirizzo IP, toccare <NTP: Primary server> o <NTP: Fallback server> e poi <edit>. Per confermare l'inserimento, toccare <ok>.
4. Toccare <save> e confermare per accettare e salvare le modifiche. Le impostazioni del server NTP sono abilitate.
5. Riavviare il sistema (vedere sezione 8.7 'Spegnimento').

10
Gestione degli utenti

10.1 Informazioni generali

Il sistema di gestione degli utenti del software supporta l'autenticazione degli utenti e il controllo degli accessi in base ai ruoli, in conformità con 21 CFR Parte 11.

- Autenticazione degli utenti: per effettuare il login e usare lo strumento sono necessari il nome utente (definito anche ID account) e la password. Sono supportati sia User Management in locale che l'autenticazione LDAP.
- Controllo degli accessi basato sui ruoli: gli utenti con ruoli differenti hanno differenti diritti di accesso. Il controllo degli accessi basato sui ruoli è definito in tre termini: diritti, ruoli e account.

Diritti

I diritti rappresentano l'unità minima di azione che l'utente può effettuare. I diritti sono definiti dal software e l'utente può solo raggruppare i diritti esistenti. Per una panoramica dei diversi diritti previsti nel software, vedere la Tabella A.1 nell'Appendice.

Ruoli

I ruoli rappresentano le mansioni lavorative o responsabilità all'interno di un'organizzazione. A un ruolo può essere assegnato un insieme di diritti. Il software prevede ruoli predefiniti e i principali sono elencati nella Tabella 10.1. Il software supporta ruoli personalizzati.

Account

Gli account rappresentano i singoli utenti. In un ambiente GMP deve esserci una relazione uno-a-uno tra individuo e ID account. Al momento dell'installazione, verrà creato un account amministratore con tutti i ruoli, per permettere all'utente di creare nuovi ruoli e nuovi account a seconda delle necessità.

Ruolo	Strumenti/Diritti
Application x.x operator (Applicazione x.x operatore)	Autorizzazione per l'esecuzione di questa applicazione con numero di versione x.x
ATS user (Utente ATS)	Accesso a Audit Trail, incl. visualizzazione, esportazione ed eliminazione
Administration tools user (Utente degli strumenti di amministrazione)	Accesso agli strumenti per l'amministrazione dello strumento. Suggerito per gli amministratori
Common tools user (Utente strumenti comuni)	Accesso agli strumenti comuni: Info, License, Shutdown e User Settings. Suggerito per tutti gli utenti
File management user (Utente della gestione file)	Accesso agli strumenti Backup Filed Data e Custom Files. Abilita l'accesso al logfile tramite FTP
Gas mix tool v1.0 Operator (Strumento Gas mix v1.0 Operatore)	Accesso allo strumento Gas mix
Injected programs (Programmi aggiunti)	Autorizzazione all'esecuzione di programmi aggiunti
N_2 settings tools user (Utente strumento impostazioni N_2)	Strumento che consente l'accesso alle N_2 settings (impostazioni N_2)
Set time user (Imposta ora utente)	Consente di impostare l'ora
Support tools user (Utente degli strumenti di supporto)	Accesso agli strumenti Chamber in, Chamber out, Sealer e Instrument Check
UM Administrator	Accesso a User Management che consente di gestire gli account
UM user (Utente ATS)	Operatore definito che deve avviare ed eseguire le applicazioni utente

Tabella 10.1: Panoramica dei ruoli predefiniti

Di seguito è riportato un esempio di configurazione convenzionale dell'UMS:

- L'amministratore gestisce gli account e lo strumento. Il ruolo di amministratore prevede in genere la configurazione e la modifica degli account e fornisce l'accesso alla gestione dei file e agli strumenti avanzati per la definizione delle impostazioni dello strumento.
- L'operatore avvia ed esegue le applicazioni sullo strumento. L'account di

operatore viene configurato per consentire l'esecuzione di un particolare insieme di applicazioni e strumenti, in base a quanto deciso dal cliente per il supporto e la risoluzione dei problemi nell'ambito della gestione degli utenti. I tipi di utente definiti dal cliente possono essere molteplici, e a ciascun utente possono essere assegnati uno o più ruoli.

IMPORTANTE

A un operatore deve essere assegnato il ruolo 'UM User'. A un amministratore deve essere assegnato il ruolo 'UM Administrator'.

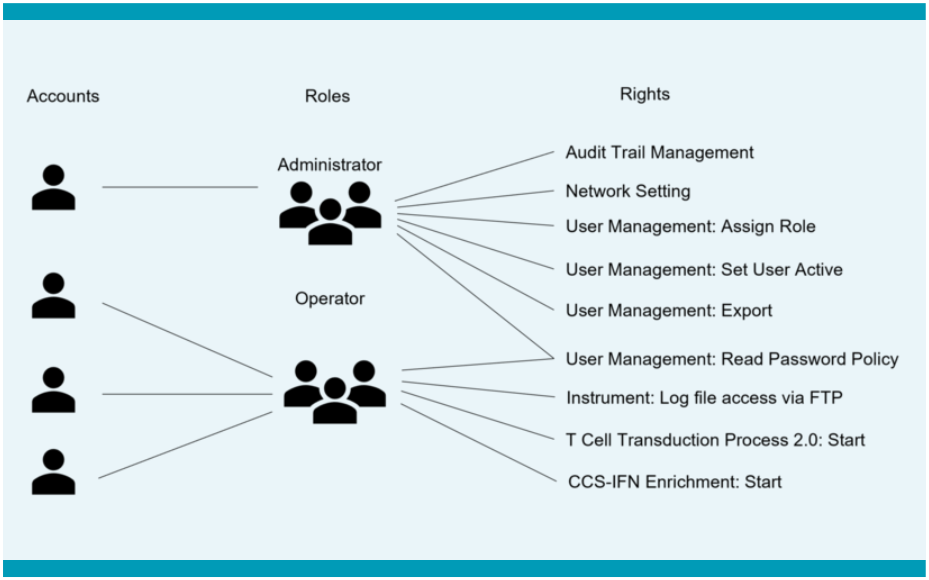


Figura 10.1: Parametri di connessione esemplificativi

⚠ ATTENZIONE

Rischio di interruzione del processo a causa di un login non riuscito. Se non si riesce più a effettuare il login, vi è il rischio di un'interruzione del processo. Per evitare questa situazione, prima di avviare un'applicazione sullo strumento è necessario creare degli account utente e amministratore appropriati con password distinte. Qualora non sia più possibile effettuare il login allo strumento, contattare Miltenyi Biotec Technical Support.

IMPORTANTE

- Si consiglia vivamente di preparare una soluzione di emergenza per le situazioni di emergenza, come un account amministratore aggiuntivo da utilizzare in caso di emergenza. Le credenziali per l'account di emergenza devono essere conservate in un luogo sicuro e devono essere accessibili solo a determinate persone.
- La procedura di autenticazione deve essere descritta e implementata

nell'ambito del sistema di gestione della qualità della struttura e tutti gli utenti e gli amministratori devono essere addestrati in merito.

- Se la connessione LDAP non funziona, utilizzare un account utente locale per accedere allo strumento.

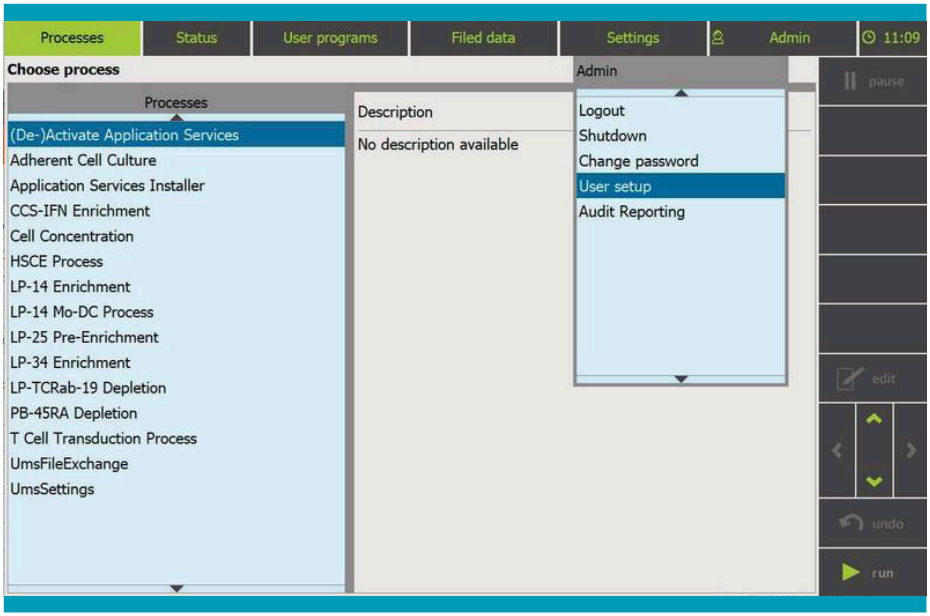
10.2 Gestione di ruoli e account

IMPORTANTE

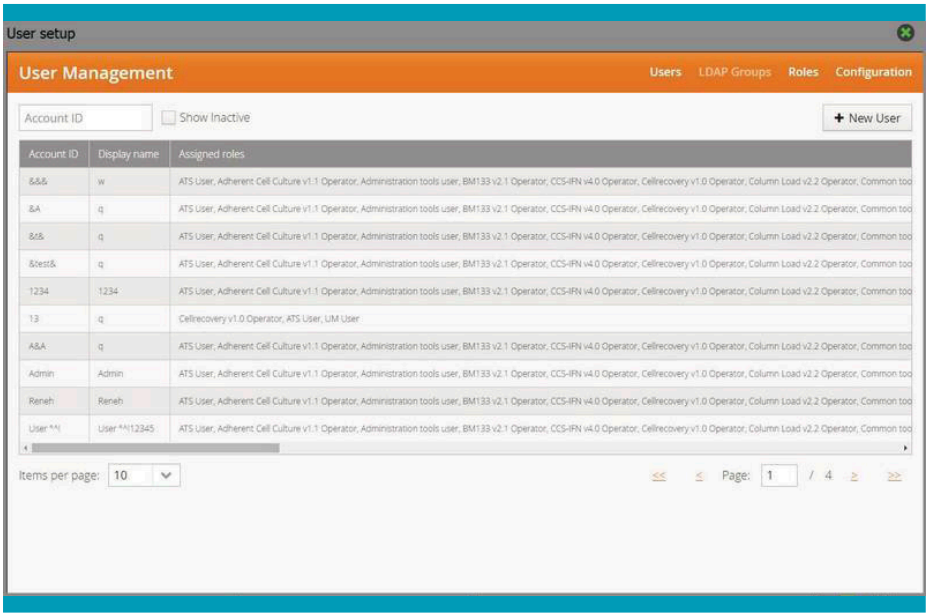
Per configurare il sistema di gestione degli utenti, un utente deve avere un ruolo 'UM Administrator'.

10.2.1 Accesso a User Management

Per accedere a User Management System, selezionare (menu di accesso rapido) e toccare **<User setup>**. Viene visualizzata la pagina User Management (Schermata 10.2). User Management ha quattro pagine: **<Users>**, **<LDAP Groups>**, **< Roles>** e **<Configuration>**. **<Users>** è selezionato di default.



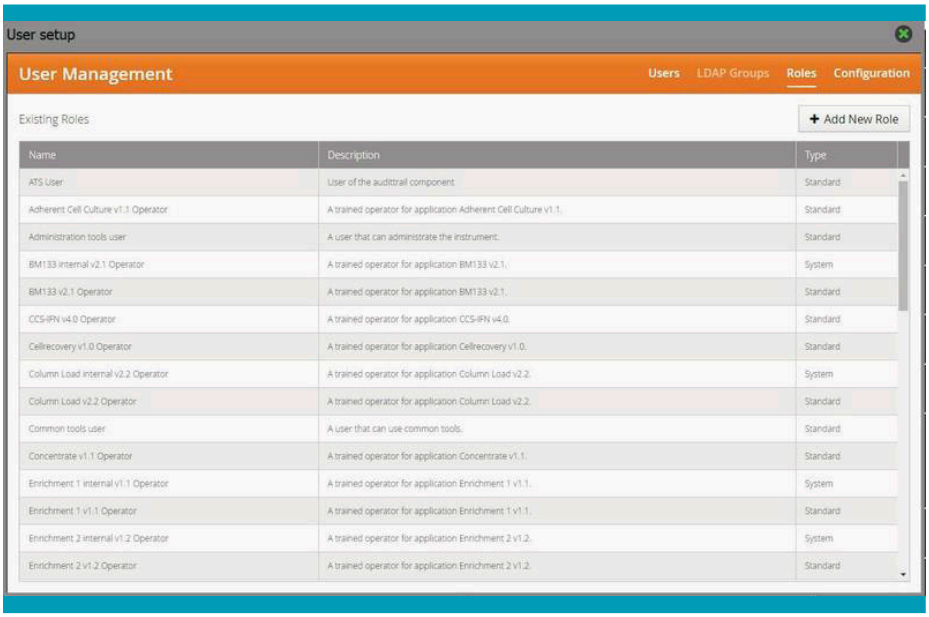
Schermata 10.1: Selezionare User setup



Schermata 10.2: Menu User Management

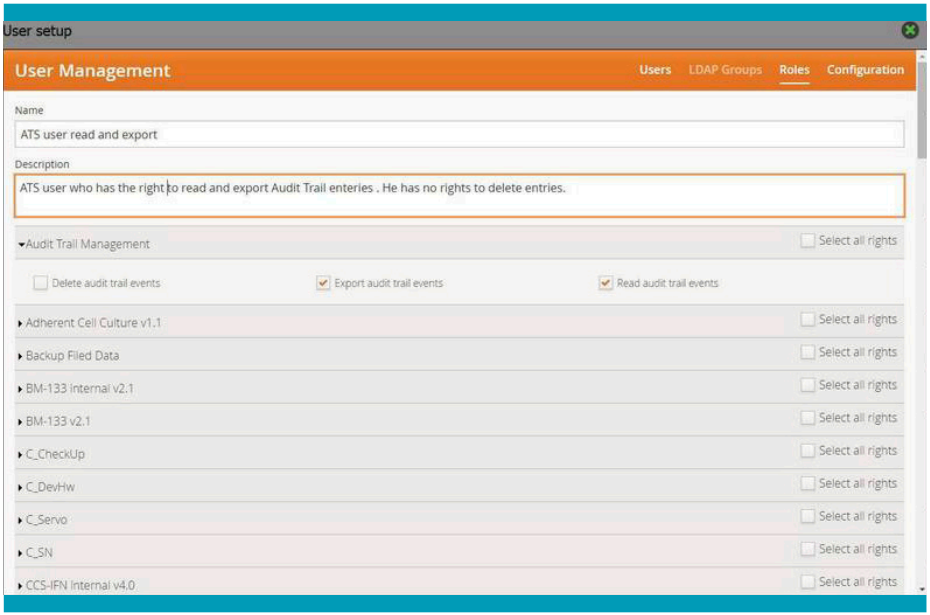
10.2.2 Creazione di un nuovo ruolo

1. Toccare <Roles> in <User Management>. Viene mostrato un elenco di ruoli esistenti (Schermata 10.3).



Schermata 10.3: Ruoli definiti in User Management

2. Toccare <+Add New Role> (Schermata 10.3). Viene visualizzata una nuova pagina per la definizione dei ruoli (vedere Schermata 10.4).



Schermata 10.4: Creazione di un nuovo ruolo

3. Inserire il nome e la descrizione del ruolo. Selezionare con una spunta iil diritto desiderato per questo ruolo.
4. Toccare <save> in fondo alla pagina. Il nuovo ruolo aggiunto viene visualizzato nell'elenco dei ruoli esistenti e può essere assegnato a un utente.

10.2.3 Modifica dei diritti assegnati ai ruoli

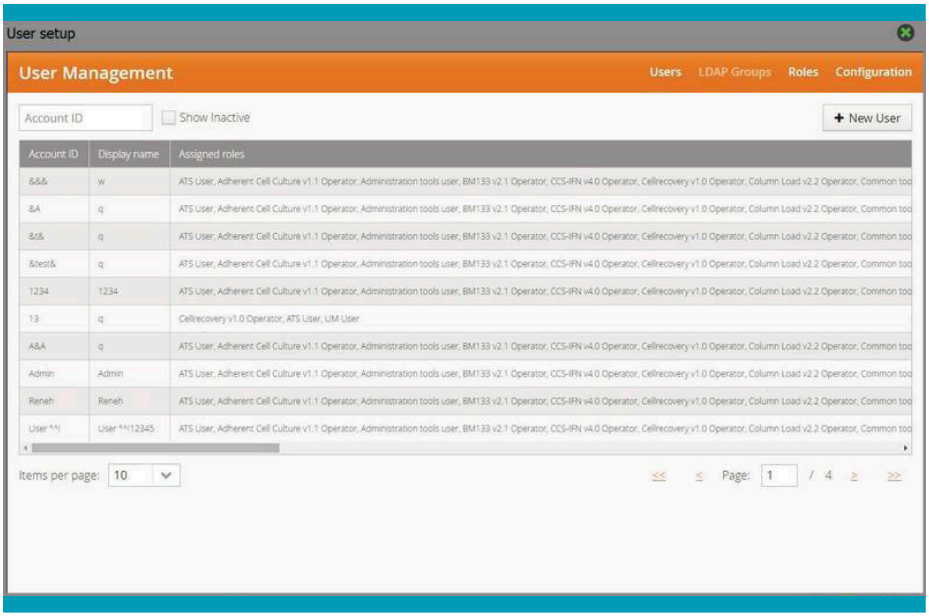
1. Trovare e selezionare il ruolo nell'elenco dei ruoli esistenti (vedere Schermata 10.3)
2. Selezionare o deselezionare i diritti desiderati.
3. Scorrere verso il basso fino in fondo e toccare <save>.

10.2.4 Aggiunta di un utente locale

IMPORTANTE

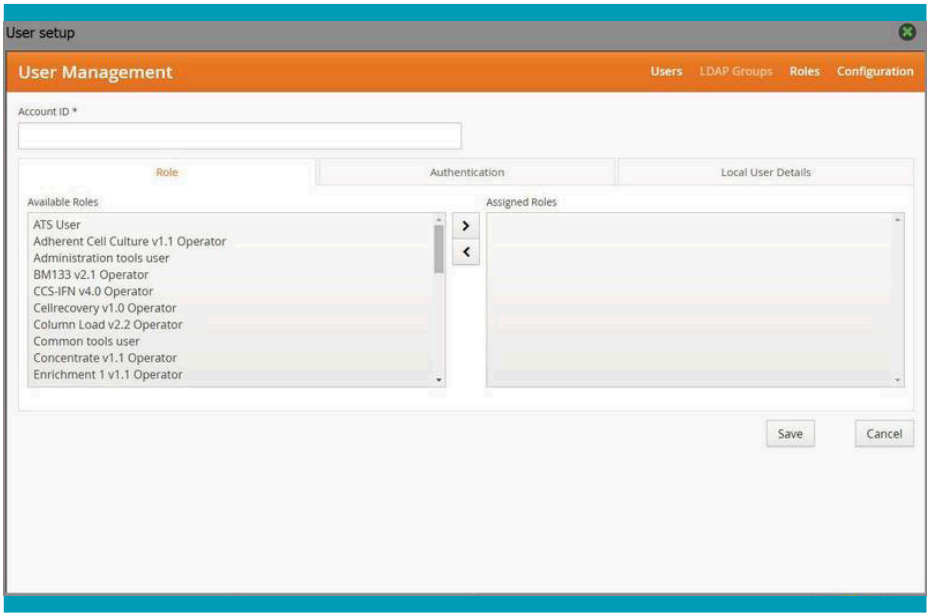
- Per creare un nuovo account, un utente deve avere il ruolo 'UM Administrator'.
- In ambiente GMP, è necessario utilizzare nomi reali o sinonimi chiaramente distinguibili e riconoscibili.

1. Selezionare il menu <Users> in User Management.
2. Toccare <+New User>. Viene visualizzata una nuova pagina utente (Schermata 10.5).



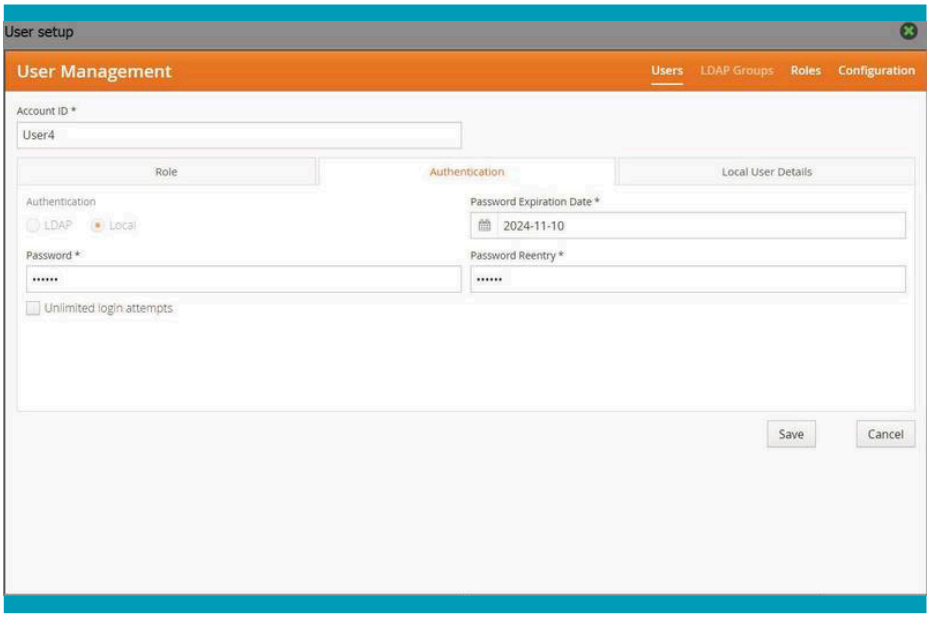
Schermata 10.5: Menu New user

3. Inserire l'ID account (Schermata 10.6). Questo ID account deve essere unico e deve essere associato a un solo utente finale. L'ID account corrisponde al nome utente inserito al login. Se Active Directory è configurato, il software controlla se questo ID è registrato nel server AD. Se l'ID account non viene trovato, verrà creato un account locale. Se viene trovato, l'account AD verrà utilizzato di default. Per modificare un account LDAP in un account locale, procedere come indicato al passaggio 5.
4. Per assegnare i ruoli corrispondenti a questo account, selezionare l'elemento in <Available Roles> nella scheda <Role> e toccare ☐ (Schermata 10.6). Per rimuovere un ruolo assegnato a questo account, selezionare l'elemento in <Assigned Roles> e toccare ☐



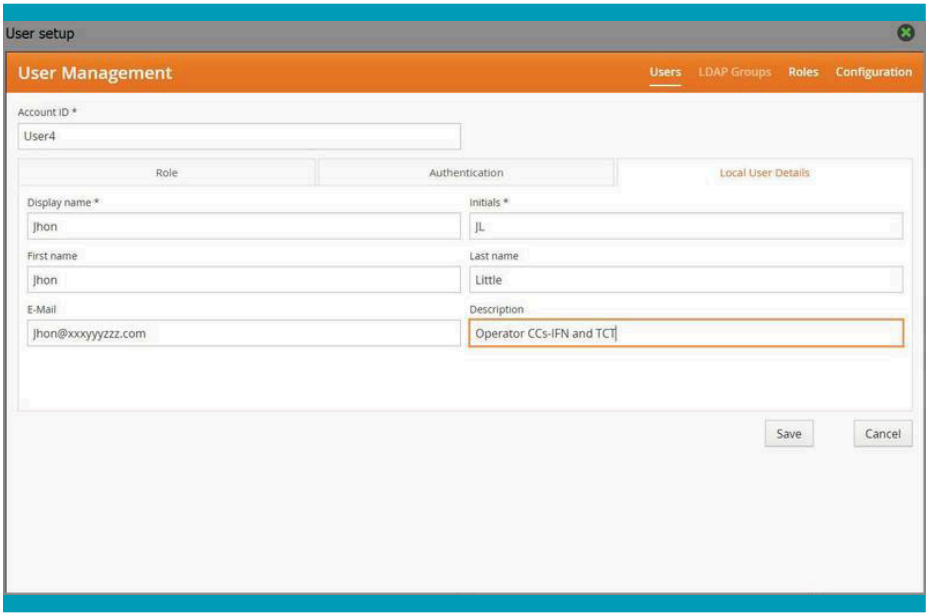
Schermata 10.6: Pagina di configurazione dell'utente

5. Se LDAP è configurato e Account ID si trova sul server AD, l'utente può scegliere tra l'autenticazione tramite il server AD o il database locale. Per un utente locale, inserire la password e impostare la durata in base ai criteri password (vedere sezione 10.3 'Configurazione dei criteri password').



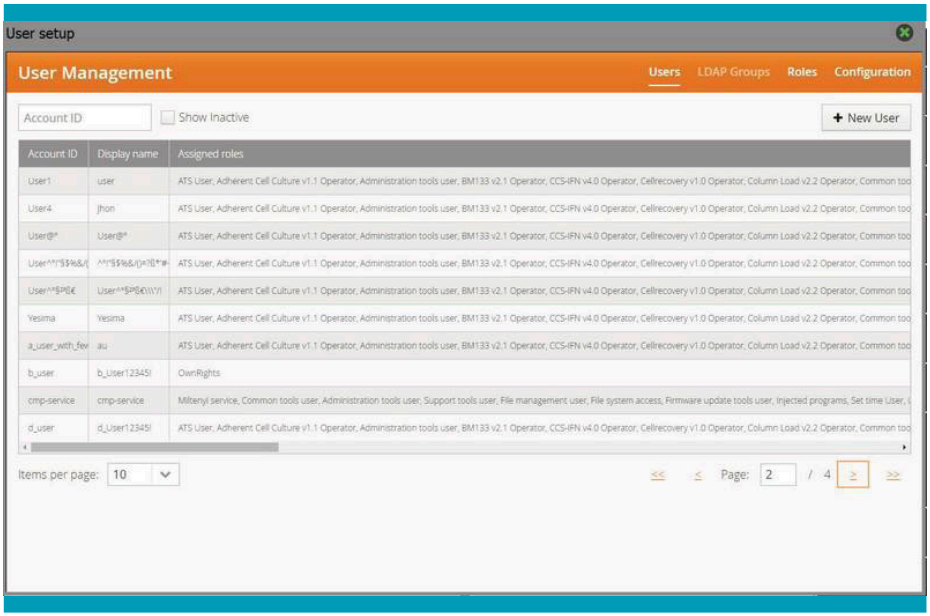
Schermata 10.7: Inserire la password del nuovo utente

6. Nella scheda <Local User Details>, impostare informazioni più dettagliate su questo account.



Schermata 10.8: Inserire i dettagli per l'utente locale

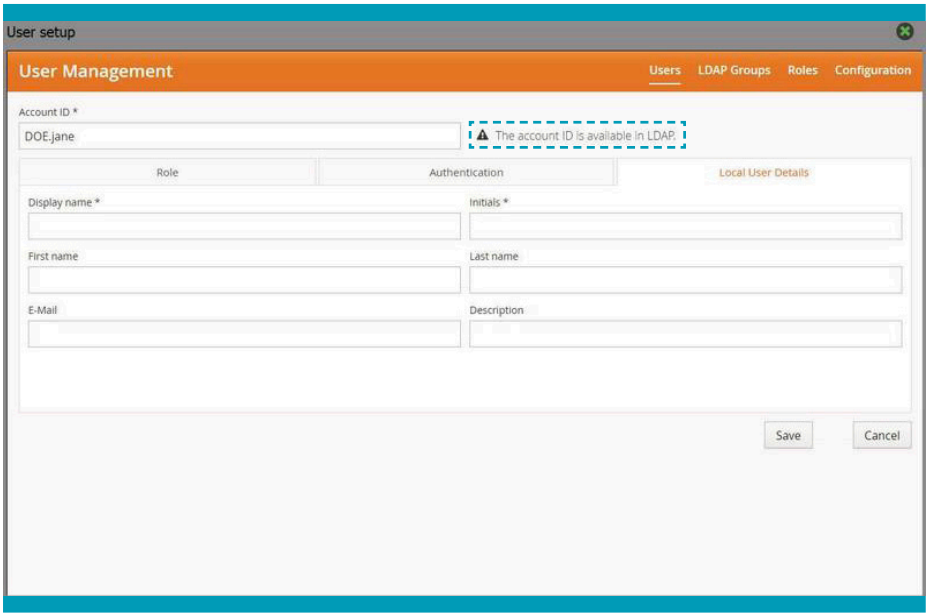
7. Toccare <save>. Il nuovo account aggiunto viene visualizzato nell'elenco degli account (Schermata 10.9).



Schermata 10.9: Conferma del nuovo utente aggiunto

10.2.5 Aggiunta di utenti LDAP

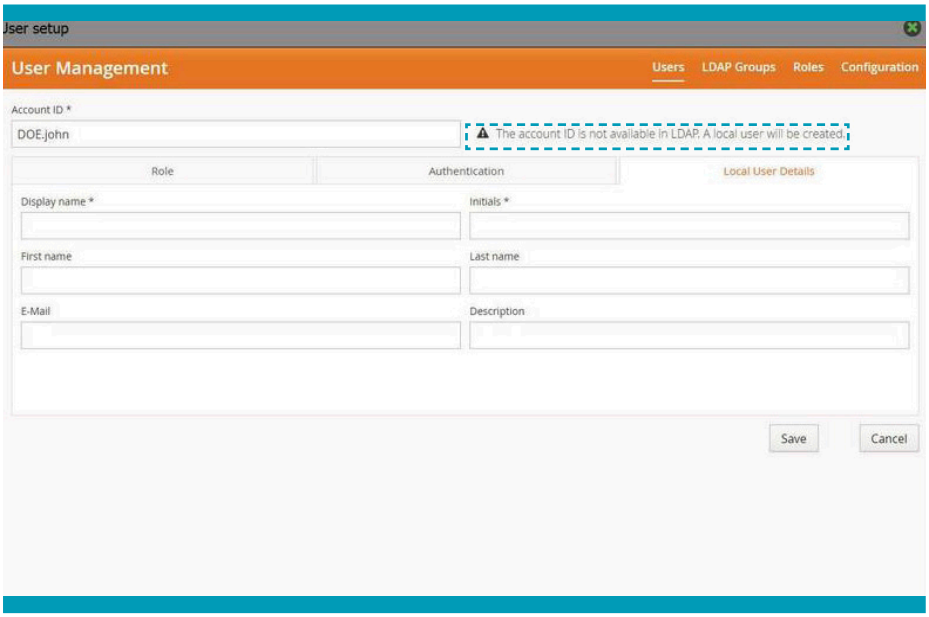
1. Selezionare <Users> in <User Management>.
2. Toccare <+New User>.
3. Inserire l'ID account LDAP. Il software controllerà se questo ID è registrato nel server AD. Se l'utente esiste già, verranno inserite ulteriori informazioni usando la mappatura degli attributi (vedere Schermata 10.10). Se l'utente non è registrato in AD, viene creato un nuovo utente locale (vedere Schermata 10.11).



Schermata 10.10: Menu User Management LDAP Users con esempio di utente non registrato

4. Per assegnare i ruoli toccare <Role> e selezionare il ruolo desiderato.

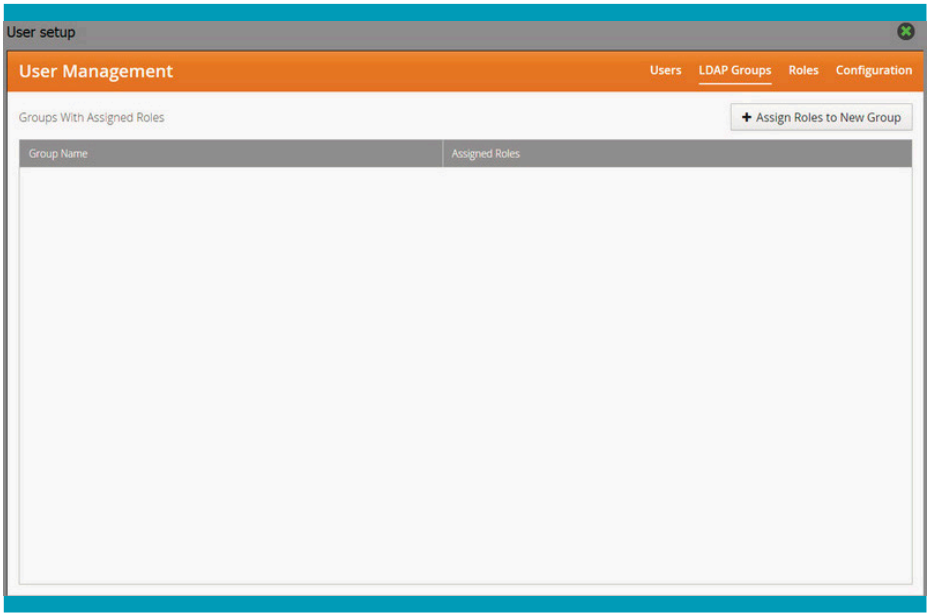
5. Toccare <save>. Per effettuare il login, l'utente può usare l'ID account e la password LDAP.



Schermata 10.11: Menu User Management LDAP Users con esempio di utente non registrato

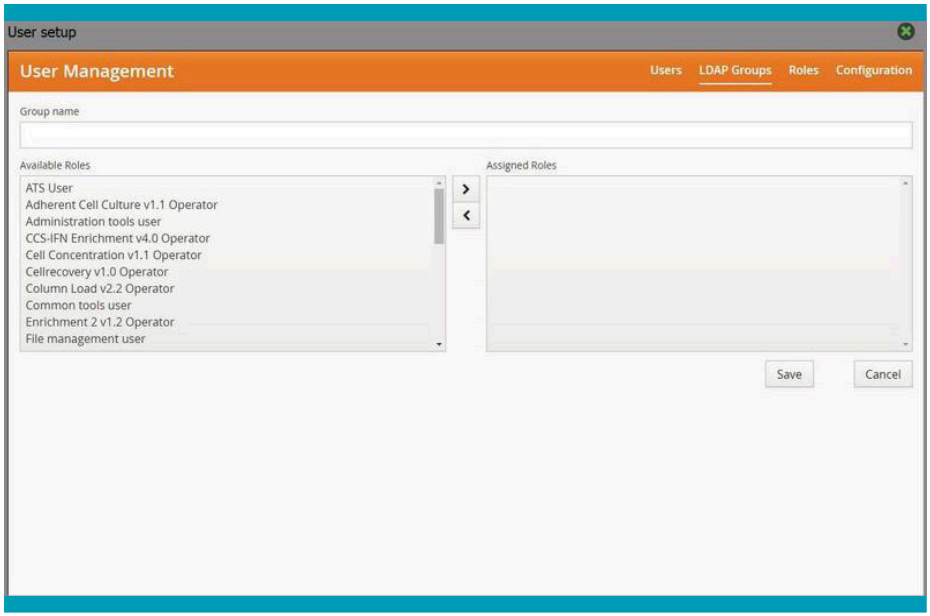
10.2.6 Aggiunta di gruppi LDAP

1. Selezionare <LDAP Groups> nella barra dei menu e toccare <+ Assign Roles to New Group>.



Schermata 10.12: Menu User Management e passaggio necessario per aggiungere gruppi LDAP

2. Inserire il nome del gruppo (vedere Schermata 10.13). Il sistema controllerà automaticamente se questo gruppo esiste in LDAP.
3. Per assegnare i ruoli a questo gruppo, selezionare i ruoli in <Available Roles> e toccare ›. Per rimuovere un ruolo assegnato a questo gruppo, selezionare l'elemento in <Assigned Roles> e toccare ‹
4. Toccare <save>.



Schermata 10.13: Menu User Management LDAP user groups

IMPORTANTE

Per effettuare correttamente il login, assicurarsi di aggiungere il corretto 'UM Administrator' o 'UM User'.

10.2.7 Modifica dei ruoli assegnati a un utente o a un gruppo LDAP

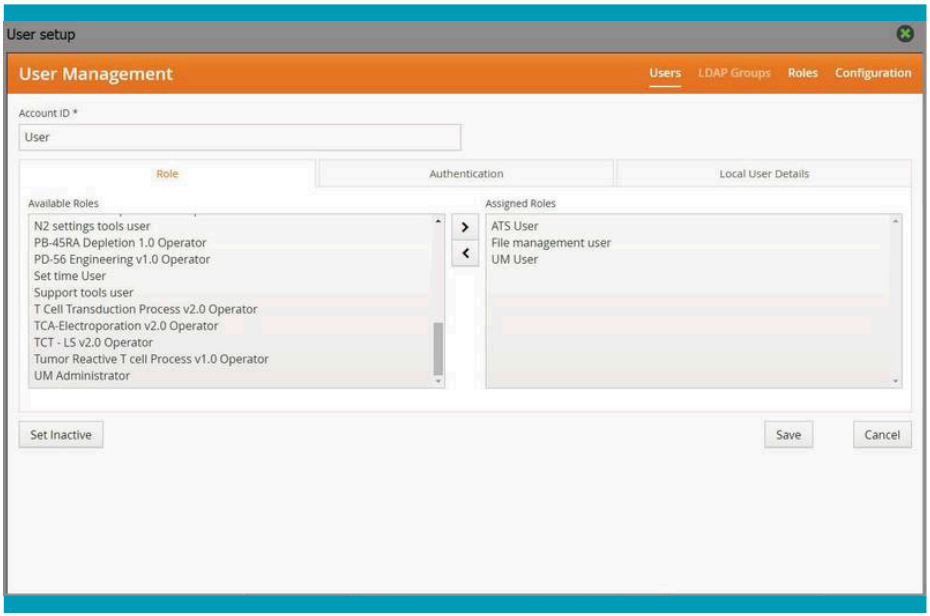
1. Selezionare l'utente nell'elenco degli utenti nella pagina Users (Schermata 10.2) e toccare l'elemento. Per il gruppo LDAP, selezionare il gruppo desiderato nella pagina LDAP groups (gruppi LDAP, vedere la Schermata 10.12).
2. Per assegnare ruoli aggiuntivi all'utente, selezionare l'elemento in **<Available Roles>** nella scheda **<Role>** e toccare ›. Per rimuovere i ruoli assegnati a questo account, selezionare l'elemento in **<Assigned roles>** e toccare la scheda ‹
3. Toccare **<Save>** in basso nella scheda **<Role>**.

10.2.8 Disattivazione utenti locali

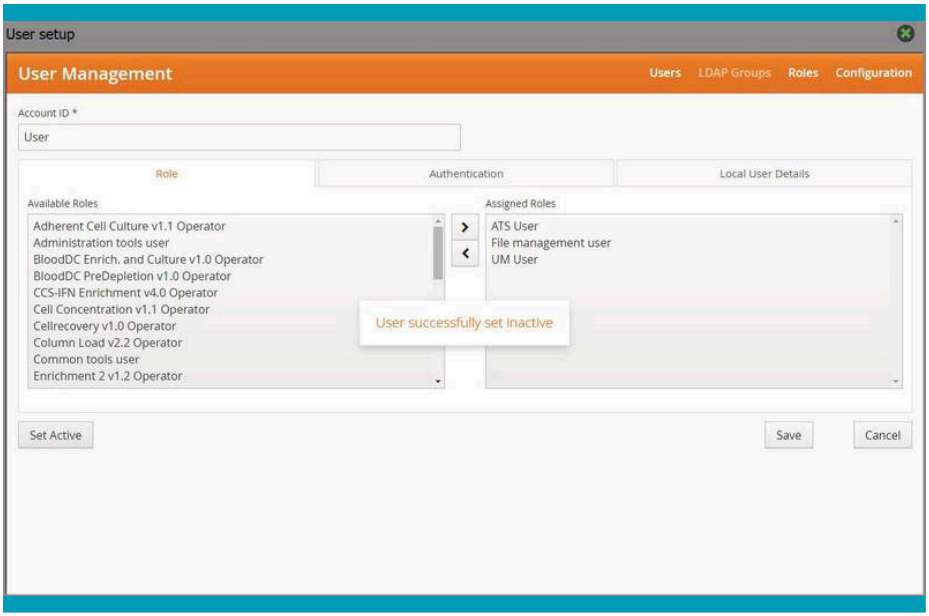
Nota: l'utente locale può essere disattivato ma non eliminato.

1. Selezionare l'utente locale dall'elenco degli utenti (Schermata 10.9). Si apre la pagina User Configuration.

2. Toccare <Set Inactive> in fondo alla pagina di configurazione dell'utente (Schermata 10.14).

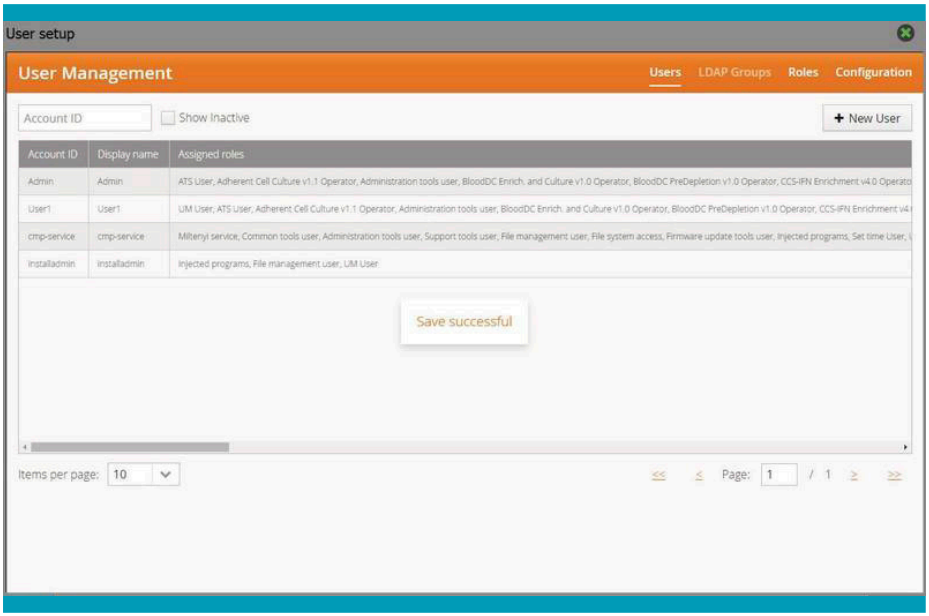


Schermata 10.14: Impostazione di un utente locale inattivo



Schermata 10.15: Utente impostato come inattivo

3. Toccare <Save> in basso per tornare all'elenco degli utenti.

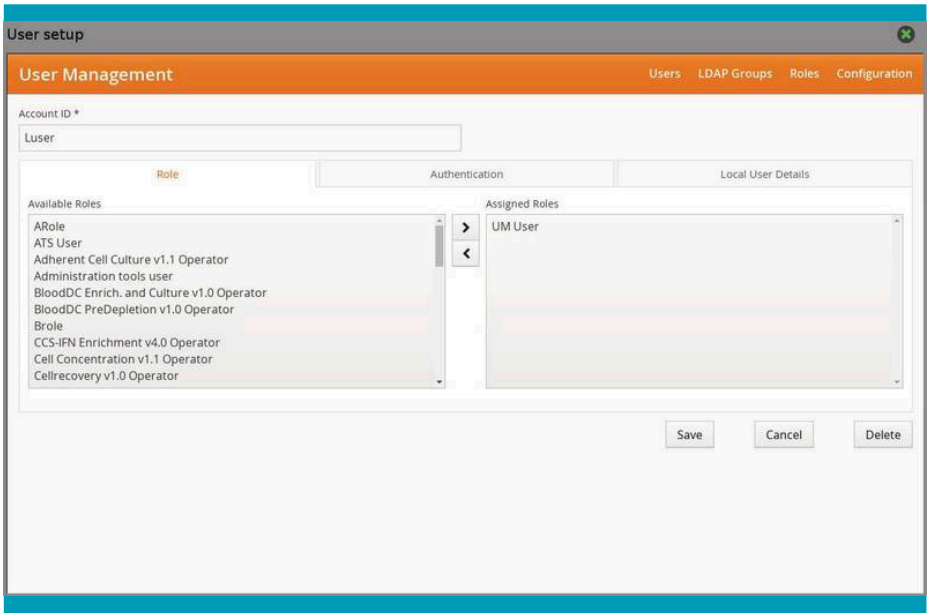


Schermata 10.16: Salvataggio andato a buon fine

L'account inattivo non viene visualizzato nell'elenco degli utenti. Tuttavia l'account è ancora archiviato sullo strumento. Per visualizzare o riattivare l'account, selezionare <Show Inactive> (vedere Schermata 10.16) e procedere come indicato nella sezione 10.2.7 'Modifica dei ruoli assegnati a un utente o a un gruppo LDAP'.

10.2.9 Eliminazione utenti LDAP

1. Selezionare un utente LDAP o un gruppo LDAP dall'elenco degli utenti.
2. Nella pagina di configurazione dell'utente, toccare <Delete> (vedere Schermata 10.14).



Schermata 10.17: Eliminazione l'utente LDAP

3. Toccare <Save> in basso per tornare all'elenco degli utenti.

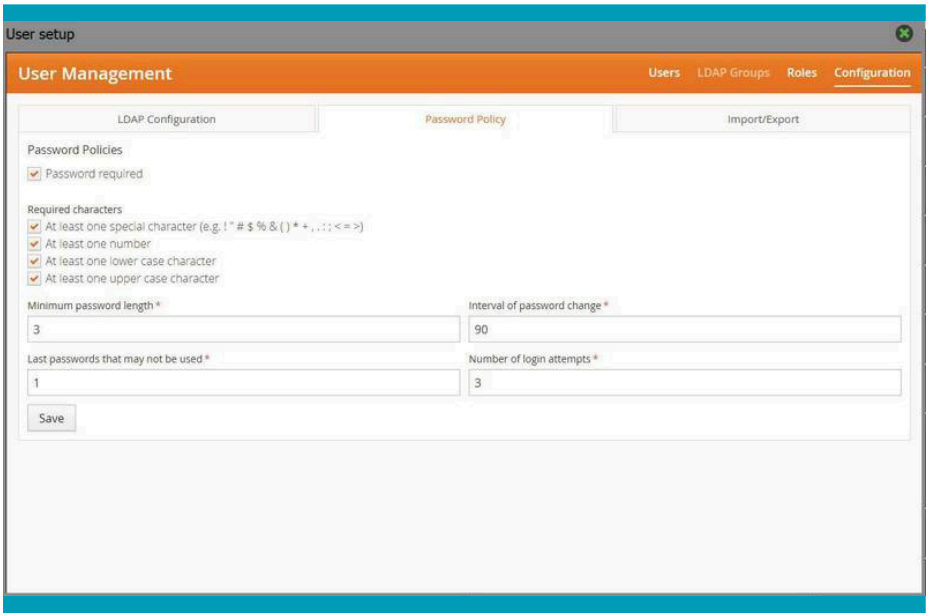
10.3 Configurarazione dei criteri password

Per configurare i criteri password, toccare <Configuration> (configurazione) nell'angolo in alto a destra e selezionare la scheda <Password Policy>. È possibile configurare quanto segue:

- Caratteri necessari
- Lunghezza della password
- Durata della password (in giorni)
- Ultime password che non possono essere utilizzate
- Numero massimo di tentativi di login

Nota: la modifica dei criteri password avrà effetto solo su utenti creati successivamente e non influirà sugli utenti già creati.

Nota: i criteri password vengono sovrascritti dai criteri password LDAP per l'account LDAP.



Schermata 10.18: Configurazione dei criteri password

10.4 Impostazioni di Import ed Export in User Management

La configurazione di UMS può essere trasferita da uno strumento all'altro. Il processo prevede due fasi:

(1) Copia tra la penna USB e la cartella di scambio UMS utilizzando lo strumento UMS Exchange

(2) Importazione/Esportazione in UMS nella configurazione User Management.

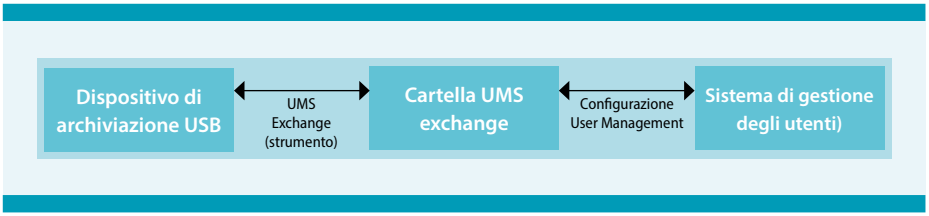


Figura 10.2: User Management System (Sistema di gestione degli utenti)

La procedura di esempio si applica a entrambi i file seguenti:

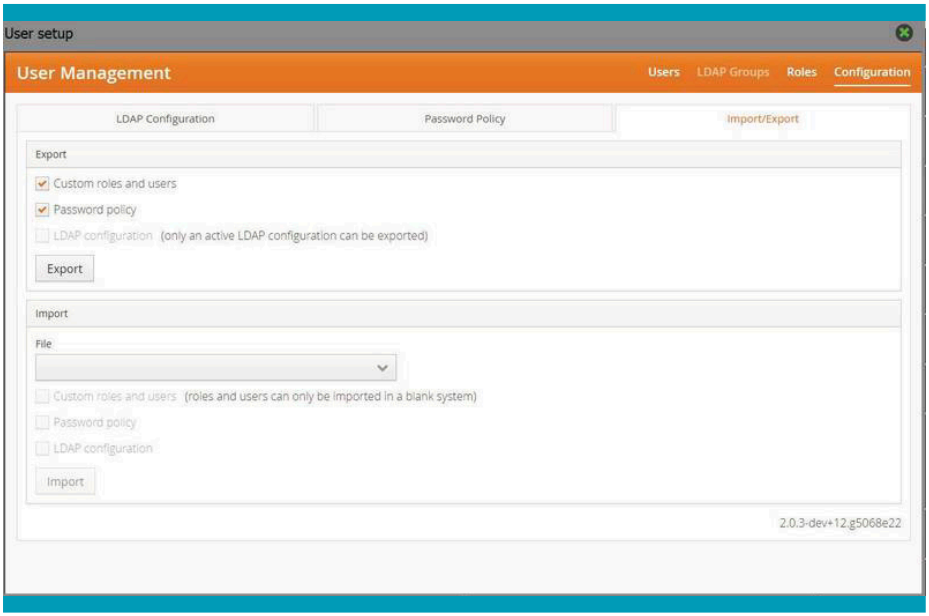
- Importare i file dei certificati Secure Sockets Layer (SSL) per configurare una connessione LDAP sicura.
- Importare ed esportare i file UMS Settings per il backup o il riutilizzo in altre istanze UMS.

Nota: solo gli utenti UMS con ruolo di amministratore 'Administration tools user' possono accedere a questa applicazione.

10.4.1 Impostazioni di Export in User Management

IMPORTANTE
I ruoli e gli utenti possono essere importati solo in un sistema vuoto.

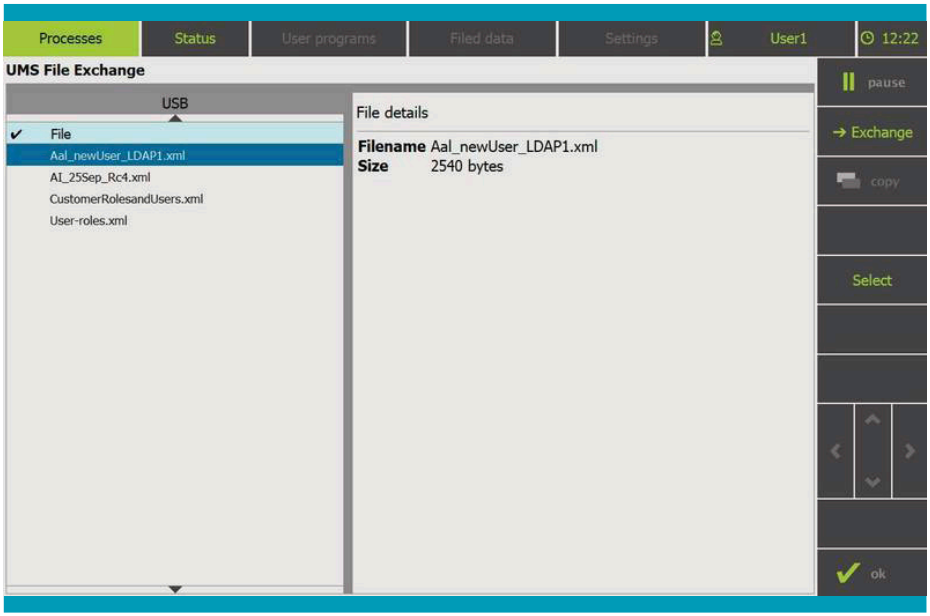
1. Inserire una penna USB.
2. Selezionare **<User Management>** ▸ **<Configuration>** ▸ **<Import/Export>**. Toccare **<Export>**. Le impostazioni UMS vengono esportate nella cartella UMS Exchange dello strumento.



Schermata 10.19: Sottomenu 'Configuration' (configurazione) con 'Import/Export' attivo

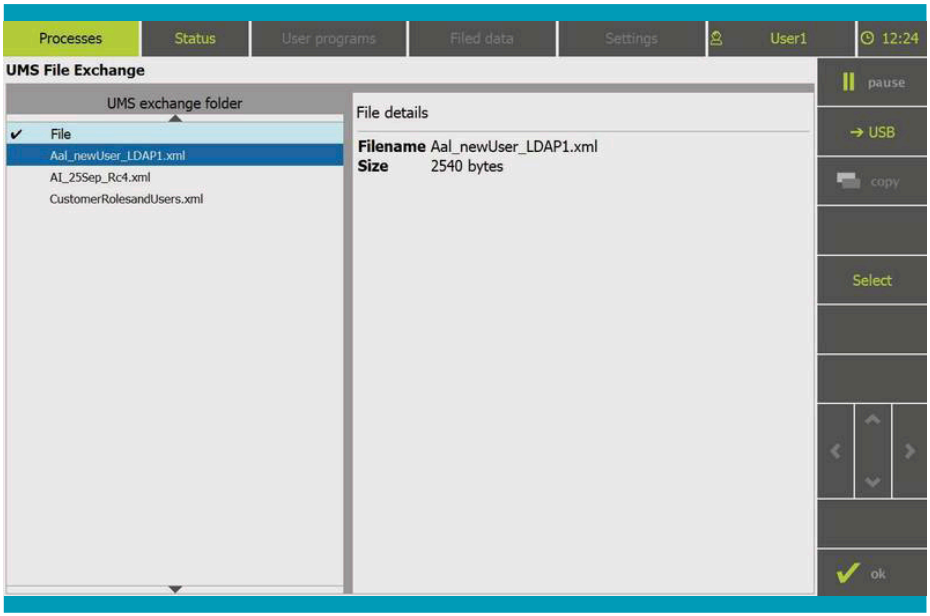
3. Per accedere a <UMS File Exchange>, selezionare <Settings> ▸ <Tools>, < UMS File Exchange> e toccare <run>.

4. Se USB è visualizzato nella colonna a sinistra, toccare <Exchange> per elencare il contenuto della cartella UMS Exchange (vedere Schermata 10.20). I file presenti nella cartella UMS Exchange verranno visualizzati nella colonna a sinistra (vedere Schermata 10.21).



Schermata 10.20: File selezionato e pulsante di menu 'Exchange'

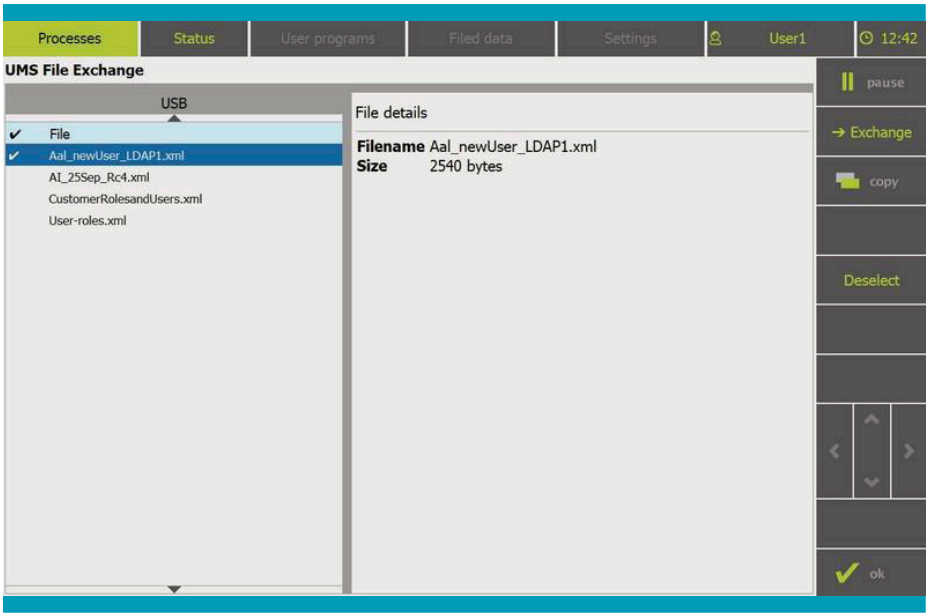
5. Selezionare i file da trasferire in UMS e toccare <Select>.
6. Una volta selezionati tutti i file da trasferire, toccare <copy> per avviare il trasferimento.



Schermata 10.21: Cartella UMS Exchange con file selezionati

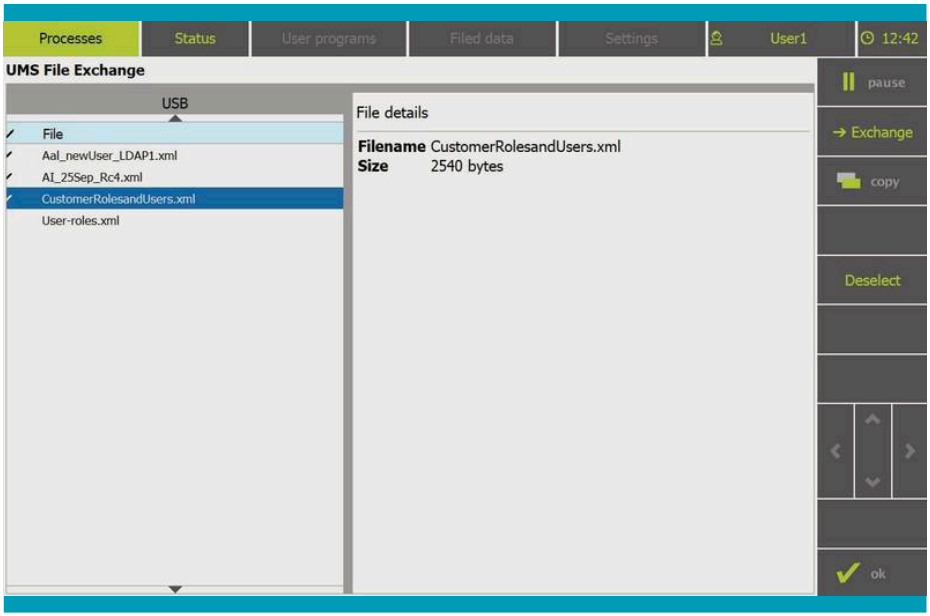
10.4.2 Importazione impostazioni in UMS

1. Inserire una penna USB.
   Assicurarsi che i file si trovino nella cartella di primo livello della penna USB (i file presenti nelle sottocartelle non verranno riconosciuti).
2. Selezionare <Process> ▸ <Tools>, <UMS File Exchange>, toccare <run> per accedere allo strumento <UMS File Exchange>. Un elenco di file viene visualizzato a sinistra.
3. Quando viene visualizzata la cartella UMS Exchange, toccare <USB> nella barra degli strumenti. Assicurarsi che <USB> sia visualizzato sopra l'elenco dei file nella colonna a sinistra.
4. Selezionare i file da trasferire e toccare <Select>. Per deselezionare un file, scegliere il file selezionato e toccare < Deselect >.



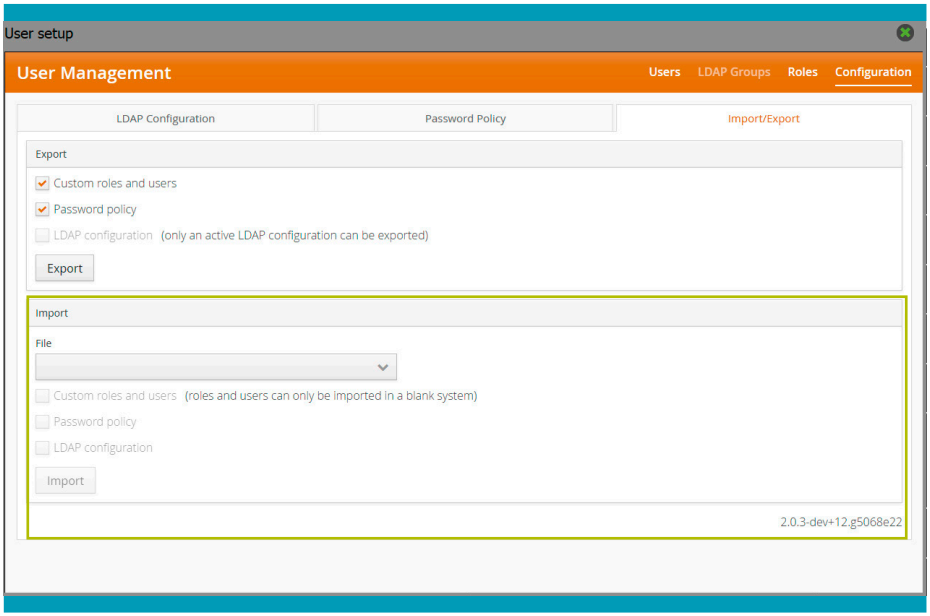
Schermata 10.22: File selezionato e pulsante di menu 'Select'

5. Una volta selezionati tutti i file da trasferire, toccare <Copy> per avviare il trasferimento.



Schermata 10.23: Cartella USB con file selezionati

6. Selezionare <User setup> ▸ <Configuration> ▸ <Import/Export>. Selezionare il file in <Import> e toccare <Import>.



Schermata 10.24: Sottomenu 'Configuration' (configurazione) con scheda 'Import/Export' attiva

11 Risoluzione dei problemi

In caso di malfunzionamento o interruzione del processo, contattare il Miltenyi Biotec Technical Support:

+49 2204 8306-3803
technicalsupport@miltenyi.com

Per le informazioni di contatto del Miltenyi Biotec Technical Support locale, visitare il sito www.miltenyibiotec.com.

12 Note legali

12.1 Garanzia limitata

Fatta eccezione per quanto indicato in una dichiarazione di garanzia specifica, che può accompagnare questo prodotto di Miltenyi Biotec, o salvo diversamente convenuto per iscritto da un rappresentante di Miltenyi Biotec debitamente autorizzato, la garanzia di Miltenyi Biotec per i prodotti acquistati direttamente da Miltenyi Biotec sarà soggetta ai termini e alle condizioni di vendita previsti dalla rispettiva organizzazione di vendita di Miltenyi Biotec. Questi termini e condizioni sono disponibili su richiesta o all'indirizzo www.miltenyibiotec.com. I termini e le condizioni di vendita applicabili possono variare in base al Paese e all'area geografica. Nulla di quanto qui contenuto può essere interpretato come garanzia aggiuntiva.

Per i prodotti acquistati presso distributori o rivenditori terzi (ad esempio, acquistati presso un fornitore di servizi autorizzato Miltenyi Biotec locale) potrebbero applicarsi termini e condizioni diversi.

Per stabilire la garanzia fornita con il prodotto, consultare il documento di trasporto, la fattura, la ricevuta o altra documentazione di vendita. Alcuni componenti di una combinazione di prodotti acquistati potrebbero avere una garanzia più breve di quella riportata sul documento di trasporto, sulla fattura, sulla ricevuta o su altra documentazione di vendita (ad esempio prodotti soggetti a scadenza e obsolescenza).

La garanzia di Miltenyi Biotec per questo prodotto copre unicamente problemi dovuti a difetti di materiali o di lavorazione durante il normale utilizzo. Non copre problemi legati al prodotto per qualsiasi altra causa, inclusi a titolo puramente esemplificativo quelli dovuti all'utilizzo del prodotto in modo diverso da quanto specificamente descritto in questo manuale, ad esempio: uso non appropriato o improprio; montaggio o installazione non corretti da parte di un operatore o di terzi; normale usura; uso, manipolazione, conservazione, assistenza o manutenzione negligenti o non corretti; mancata aderenza alle istruzioni operative;

modifiche non autorizzate di/a qualsiasi parte del prodotto; o uso di materiali di consumo, accessori o materiali di lavoro non appropriati.

La garanzia di Miltenyi Biotec non copre i prodotti venduti COSÌ COME SONO o CON TUTTI I DIFETTI né i materiali di consumo. Nulla di quanto qui contenuto può essere interpretato come garanzia aggiuntiva.

Miltenyi Biotec deve essere informata immediatamente nel caso in cui venga presentata una richiesta secondo i termini di tale garanzia. In caso di difetti di materiali o di fabbricazione entro il periodo di garanzia, Miltenyi Biotec adotterà le misure appropriate per ripristinare la piena usabilità dello strumento.

Limitazione relativa ai danni
Miltenyi Biotec non è responsabile per danni incidentali o indiretti dovuti alla violazione di qualsiasi condizione o garanzia esplicita o implicita su questo prodotto.

Alcuni paesi/stati o giurisdizioni non consentono l'esclusione o la limitazione ai danni incidentali o consequenziali, pertanto le limitazioni o le esclusioni di cui sopra potrebbero non essere applicabili. La presente dichiarazione di garanzia riconosce specifici diritti legali e l'utilizzatore potrebbe disporre di altri diritti, che variano da Stato a Stato o da giurisdizione a giurisdizione.

12.2 Marchi commerciali

CliniMACS, CentriCult e il logo Miltenyi Biotec sono marchi registrati o marchi depositati di Miltenyi Biotec e/o sue affiliate in vari paesi in tutto il mondo.

APPENDICE

Ogni singolo processo, strumento e impostazione sono associati a diritti specifici, ad es. il diritto 'Show' o 'Start'. Un ruolo con diritto 'Show' può visualizzare lo strumento/il processo/l'impostazione nella scheda Process/Settings. Per eseguire il processo/lo strumento/l'impostazione, il ruolo deve disporre del diritto 'Start'. I componenti più complessi quali audit trail e user management hanno diritti più dettagliati.

Processo/Strumento/Impostazioni/ Componente	Dettagli
Process xxx right (Diritto per processo xxx)	• Show process xxx (Mostra processo xxx) • Start process xxx (Avvia processo xxx)
Tool xxx right (Diritto per strumento xxx) • Backup Filed Data • Custom Files (File personalizzati) • Instrument check (Controllo strumento) • License (Licenza) • N2 Settings (Impostazioni N2) • Network Settings (Impostazioni di rete) • Set Time (Imposta ora) • Settings Exchange (Scambio impostazioni) • Set Volume (Imposta volume) • Spegnimento • UMS File Exchange exchange (Scambio impostazioni file UMS) • UMS Settings settings Process xxx right (Impostazioni UMS Settings Diritto su processo xxx)	• Show tool xxx (Mostra strumento xxx) • Start tool xxx (Avvia strumento xxx)
Setting xxx right (Diritto di impostazione xxx) • Info • Impostazioni di sistema	• Show setting xxx (Mostra impostazione xxx) • Start setting xxx (Avvia impostazione xxx)

Processo/Strumento/Impostazioni/ Componente	Dettagli
Instrument (Strumento)	• Log file access via FTP (Accesso al logfile tramite FTP) • Show injected programs (Mostra programmi aggiunti) • Start injected programs (Avvia programmi aggiunti)
User Management (Gestione utenti)	• Assegnazione di ruoli • Configure LDAP connection (Configura connessione LDAP) • Creazione di ruoli • Create user (Crea utente) • Esportazione • Importazione • Read Password Policy (Leggi criteri password) • Read details of foreign account (Leggi dettagli account terzi) • Lettura dei dettagli del proprio account • Read own user details (Leggi dettagli propri utente) • Read rights of foreign account (Leggi diritti di lettura account di terzi) • Diritti di lettura del proprio account • Ruolo di lettura • Read user details (Leggi dettagli utente) • Set user active (Imposta utente su attivo) • Set user inactive (Imposta utente su inattivo) • Unlock user (Sblocca utente) • Update Password Policy (Aggiorna criteri password) • Update own user details (Aggiorna dettagli propri utente) • Ruolo di aggiornamento • Update user details (Aggiorna dettagli utente)
Audit Trail Management (Gestione audit trail)	• Export audit trail events (Esporta eventi audit trail) • Read audit trail events (Leggi eventi audit trail) • Reset audit trail events (Ripristina eventi audit trail)

Tabella A.1: Panoramica dei diritti definiti nel software

Ruoli predefiniti

Ruoli	Strumenti/diritti
ATS User	Utente del componente audit trail • Audit trail Management (Gestione audit trail)
Administration tools user (Utente degli strumenti di amministrazione)	• Customer settings (Impostazioni del cliente) • Network settings (Impostazioni di rete) • Platform configuration settings (Impostazioni di configurazione della piattaforma) • Settings exchange (Scambio impostazioni) • Impostazioni di sistema • UMS File Exchange exchange (Scambio impostazioni file UMS)
File management user (Utente della gestione file)	Utente che utilizza strumenti per la gestione dei file • Backup Filed Data • Custom Files (File personalizzati) • Log file access via FTP (Accesso al logfile tramite FTP)
File system access (Accesso al file system)	Accesso a file eseguibili arbitrari nel file system – nessun accesso ai diritti
Support tools user (Utente degli strumenti di supporto)	Utente che può utilizzare strumenti che agevolano l'esecuzione di applicazioni • Chamber In • Chamber out • FormU Sensor • FormU Valves • FRAMrd • Gasmix Settings (Impostazioni della miscela di gas) • Instrument Check (Controllo strumento) • Module Settings (Impostazioni modulo) • Sealer (Saldatore)
UM Administrator	Amministratore del componente di gestione utenti User Management – tutti i diritti
UM Service	Service User (Utente del servizio) • User Management (Gestione utenti) – tutti i diritti
UM User	Custom User (Utente personalizzato) • User Management: Read details for own account (Gestione utente: Leggi dettagli per account proprio) • User Management: Read rights for own account (Gestione utente: Leggi diritti per account proprio)

Tabella A.2: Ruoli predefiniti



Miltenyi Biotec

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

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

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

Benelux
Miltenyi Biotec B.V.
Dellaertweg 9C
2316 WZ Leiden
Paesi Bassi
macsnl@miltenyi.com
Servizio clienti per:
Paesi Bassi
0800 4020120
0800 4020100
Belgio
0800 94016
0800 99626
Lussemburgo
800 24971
800 24984

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

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

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

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

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

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

Italia
Miltenyi Biotec S.r.l.
Via Paolo Nanni Costa, 30
40133 Bologna
Italia
+39 051 6 460 411
+39 051 6 460 499
macsit@miltenyi.com

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

Scandinavia e Paesi Baltici
Miltenyi Biotec Norden AB
Medicon Village
Scheeletorget 1
223 81 Lund
Svezia
macsse@miltenyi.com
Servizo clienti per:
Svezia
0200 111 800
+46 280 72 99
Danimarca
80 20 30 10
+46 46 280 72 99
Norvegia, Finlandia, Islanda e Paesi Baltici
+46 46 280 72 80
+46 46 280 72 99

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

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

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

www.miltenyibiotec.com

Miltenyi Biotec fornisce prodotti e servizi a livello mondiale. Visitate **www.miltenyibiotec.com/local** per trovare il contatto Miltenyi Biotec più vicino.

CliniMACS, CentriCult e il logo Miltenyi Biotec sono marchi registrati o marchi depositati di Miltenyi Biotec B.V. & Co. KG e/o sue affiliate in vari paesi in tutto il mondo. Copyright © 2026 Miltenyi Biotec e/o sue affiliate. Tutti i diritti riservati.

210-005-268/01 | Edizione: 2026-03