Miltenyi Biotec

Software CliniMACS Prodigy®

Manual del usuario



Los componentes del sistema CliniMACS, incluidos los reactivos, sets de tubos, instrumentos y el tampón PBS/EDTA se han diseñado, fabricado y examinado en un sistema de calidad certificado según la norma ISO 13485.En la UE, los componentes del sistema CliniMACS están disponibles como productos sanitarios con marca CE para su uso previsto, a menos que se indique lo contrario. En los EE. UU., el sistema CliniMACS CD34 Reagent, incluidos CliniMACS Plus Instrument, CliniMACS CD34 Reagent, CliniMACS Tubing Set TS y CliniMACS Tubing Set LS, así como CliniMACS PBS/EDTA Buffer, está aprobado por la FDA como un dispositivo de uso humanitario (HUD, por sus siglas en inglés) y autorizados por la ley federal de los EE. UU. para su uso en el tratamiento de pacientes con leucemia mieloide aguda (LMA) en la primera remisión completa. No se ha demostrado la eficacia del instrumento para esta indicación. Otros productos de la línea de productos CliniMACS están disponibles para el uso solo previa aprobación de una solicitud de nuevo fármaco en investigación (IND), de una exención de producto en investigación (IDE) o de una aprobación de la FDA. En Australia, los siguientes componentes del sistema CliniMACS Prodigy se incluyen en el Registro Australiano de Productos Terapéuticos (ARTG, por sus siglas en inglés), por lo que se aprueba su suministro: CliniMACS Prodigy, CliniMACS CD34 Reagent, sets de tubos CliniMACS Prodigy y CliniMACS PBS/EDTA Buffer. En Australia solo se podrán utilizar los productos incluidos en el ARTG. Los CliniMACS MicroBeads están previstos para uso en investigación y no para uso terapéutico o diagnóstico en seres humanos.

A menos que se indique específicamente lo contrario, los productos y servicios de Miltenyi Biotec son solo para uso en investigación y no para uso terapéutico o diagnóstico.

Copyright © 2026 Miltenyi Biotec y/o sus filiales. Todos los derechos reservados.

Ninguna parte de este manual puede ser reproducida, almacenada en un sistema de recuperación, transmitida, publicada o distribuida en forma alguna o por medio alguno, ya sea electrónico, mecánico, por fotocopia, microfilm, grabación u otros, sin el consentimiento expreso por escrito de Miltenyi Biotec; no obstante, y pese a lo anterior, los propietarios del sistema CliniMACS Prodigy pueden hacer copias solo con el fin de formar al personal en el uso y en el servicio de la unidad dentro de su empresa u organización.

CliniMACS, CentriCult y el logotipo de Miltenyi Biotec son marcas comerciales registradas o marcas comerciales de Miltenyi Biotec B.V. & Co. KG y/o de sus filiales en distintos países del mundo. Todas las demás marcas comerciales mencionadas en este manual del usuario o en cualquier documento adjunto son propiedad de sus respectivos propietarios y se utilizan únicamente con fines de identificación.

Software CliniMACS Prodigy®

Manual del usuario

Versión de software 2.2

Edición: 2026-03

210-005-264/01

MD CE 0123

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

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

www.miltenyibiotec.com

Información esencial

Este manual del usuario proporciona instrucciones, advertencias, precauciones, notas y otra información importante para el uso del software CliniMACS Prodigy. Para obtener detalles sobre la información relacionada con el instrumento, como la pantalla táctil y la configuración general, consultar el manual del usuario del instrumento CliniMACS Prodigy.

⚠ ADVERTENCIA

El manejo del sistema CliniMACS Prodigy debe ser realizado únicamente por operarios formados. Antes de poner el sistema en funcionamiento, leer atentamente y comprenda las informaciones de seguridad, las advertencias, precauciones e instrucciones para el funcionamiento correcto del CliniMACS Prodigy, que se proporcionan en las instrucciones de uso de los componentes del sistema CliniMACS Prodigy y en cualquier recomendación relativa a la seguridad publicada por Miltenyi Biotec. Estas instrucciones de uso incluyen, a título enunciativo, la información de seguridad del manual del usuario (instrumento) del CliniMACS Prodigy, capítulo 3 «Información de seguridad importante». Prestar especial atención a todas las advertencias que aparecen sobre el instrumento o que se proporcionan con los consumibles y accesorios, así como a las notas e información importante descritas en este manual del usuario. Seguir todas las instrucciones y los procedimientos en todo momento durante el funcionamiento del instrumento, asegurándose de que se respeta todas las informaciones de seguridad, advertencias, precauciones e instrucciones. Ignorar las informaciones de seguridad e informaciones importantes, las advertencias, precauciones, notas adicionales e instrucciones proporcionadas en las instrucciones de uso podría provocar un mal funcionamiento del instrumento, daños materiales, lesiones personales y/o la muerte. La seguridad del equipo puede verse comprometida si el instrumento no se utiliza de acuerdo con las instrucciones del fabricante. Conserve las instrucciones de uso para futuras consultas. Deberían mantenerse accesibles y disponibles, junto con todos los demás documentos de seguridad y de manejo, durante todo el ciclo de vida del instrumento, para todo el personal responsable de la instalación, del manejo y del mantenimiento.

Índice

1	**Introducción**	**9**
1.1	Información general	9
1.2	Información regulatoria	10
1.3	Normativas de protección de datos	10
1.4	Acerca de este manual	10
1.5	Documentos relacionados	11
2	**Glosario**	**13**
2.1	Nivel de peligro	13
2.2	Convenciones de estilo y formato	14
2.3	Glosario de símbolos y términos	14
2.3.1	Términos específicos del software	14
3	**Informaciones de seguridad importantes**	**17**
3.1	Instrucciones de seguridad para el CliniMACS Prodigy	17
3.2	Instrucciones de seguridad del software	18
4	**Ciberseguridad**	**19**
4.1	Concepto de defensa en profundidad para la seguridad	19
4.1.1	Capa de protección física	20
4.1.2	Capa de entorno de red	21
4.1.3	Capa de software del instrumento	24
4.1.4	Capa de usuario	25
4.1.5	Capa de auditoría	26
4.1.6	Capa de gestión de actualizaciones	26
4.1.7	Capa de gestión de vulnerabilidades	26
4.1.8	Capa de copia de seguridad y recuperación	26
4.1.9	Resumen de la configuración segura	27

5	**Concepto de software**	**29**
5.1	Concepto básico	29
5.2	La interfaz gráfica de usuario	31
5.2.1	Barra de menú y área de contenidos	31
5.2.2	Barra de estado	32
5.2.3	Barra de herramientas	33
5.2.4	Campos de entrada	34
5.2.5	Ventanas emergentes	35
6	**Manejo básico**	**37**
6.1	Encendido del instrumento	37
6.2	Inicio de sesión	38
6.3	Cierre de sesión	39
6.4	Apagado	39
6.5	Parada de emergencia	39
6.6	Seleccionar un proceso de aplicación	40
6.7	Ejecutar un proceso de aplicación	41
6.8	Pausar un proceso de aplicación	42
6.9	Estado del instrumento y del proceso de aplicación	43
6.10	Adquisición de imágenes	44
6.10.1	Cámara de detección de capas	45
6.10.2	Camera del microscopio	46
7	**Acceso a los datos**	**47**
7.1	Recuperación de registros de aplicaciones	47
7.1.1	Visualización y exportación de archivos de registro a USB	47
7.1.2	Recuperación por medio de FTP	49
7.1.3	Recuperar archivos a través de compartir archivos (File sharing)	50
7.2	Recuperación del audit trail	51
7.2.1	Ver el audit trail	52
7.2.2	Exportar el audit trail	53
7.2.3	Eliminación de un audit trail	55

8	**Herramientas y ajustes del usuario**	**57**
8.1	Acceso a herramientas y ajustes de usuario	57
8.2	Tools (Herramientas)	58
8.2.1	Info tool (Información herramientas)	58
8.2.2	Backup Filed Data (Copia de seguridad de los archivos)	59
8.2.3	Chamber In (Introducir cámara)	63
8.2.4	Chamber Out (Extraer cámara)	63
8.2.5	Shutdown (Apagar)	63
8.2.6	Recovery (Recuperación)	64
8.2.7	Herramienta Gas Mix (Mezcla de gases)	64
8.2.8	Herramienta Instrument Check (Chequeo del instrumento)	64
8.2.9	Column Load (Carga columna)	64
8.2.10	Custom Files (Archivos personalizados)	65
8.2.11	Sealer (Sellador)	65
8.3	User settings (Ajustes de usuario)	65
8.3.1	Set time (Ajustar hora)	65
8.3.2	Network settings (Ajustes de red)	65
8.3.3	Custom settings (Ajustes personalizados)	65
8.3.4	Module Settings (Ajustes del módulo)	66
8.3.5	Herramienta Settings exchange (Ajustes del intercambio)	67
8.3.6	SetVolume (Ajustar el volumen)	70
8.3.7	N_2 Settings (Ajustes N_2)	70
9	**Integración en la red**	**71**
9.1	Conexión a una red local	72
9.2	Conexión a un servidor LDAP	74
9.3	Conexión a una unidad de red	77
9.4	Configuración de la transferencia de archivos por FTP	80
9.4.1	Configuración del instrumento	81
9.4.2	Conexión con el cliente FTP	82
9.5	Conexión a un servidor de correo electrónico	83
9.6	Activación de la sincronización horaria de la red	88

10 Administración de usuarios 91

10.1 Información general 91
10.2 Administrar funciones y cuentas 94
10.2.1 Acceso a la administración de usuarios 94
10.2.2 Crear una nueva función 95
10.2.3 Cambiar los derechos de las funciones 96
10.2.4 Agregar un usuario local 96
10.2.5 Agregar usuarios LDAP 100
10.2.6 Agregar grupos LDAP 102
10.2.7 Cambiar las funciones asignadas a un usuario o grupo LDAP 103
10.2.8 Desactivar usuarios locales 103
10.2.9 Eliminación de usuarios LDAP 105
10.3 Configuración de la política de contraseñas 106
10.4 Importar y exportar ajustes de administración de usuarios 107
10.4.1 Exportar ajustes de administración de usuarios 108
10.4.2 Importar ajustes del UMS 110

11 Resolución de problemas 113

12 Aviso legal 115

12.1 Garantía limitada 115
12.2 Marcas comerciales 116

APÉNDICE

1 Introducción

1.1 Información general

El software del CliniMACS Prodigy incluye el software básico y varios programas de aplicación.

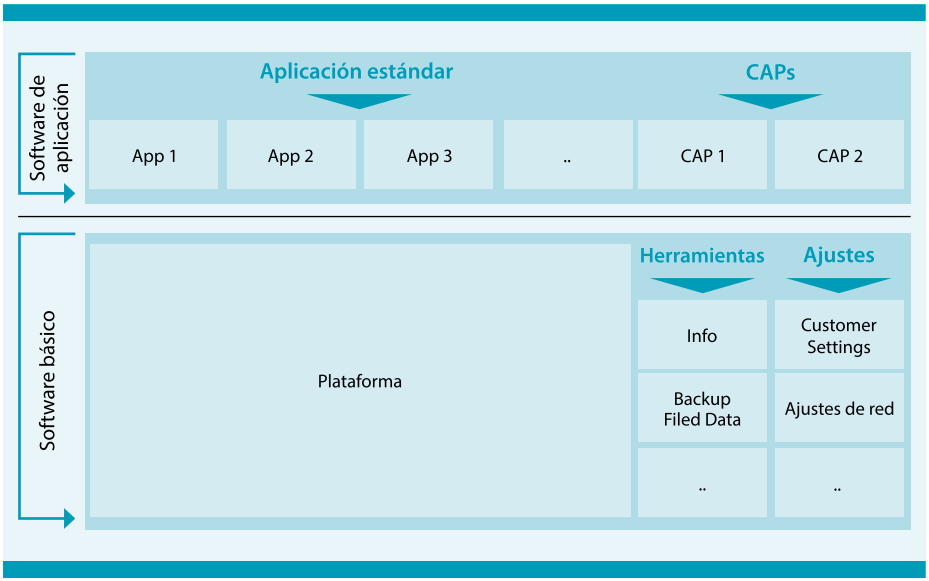


Figura 1.1: Descripción general del software del instrumento

El software básico controla el instrumento y la ejecución de los procedimientos de aplicación y proporciona servicios esenciales, tal y como se describe en los diferentes capítulos y secciones.

En este manual del usuario, el software básico también se denomina «software».

El software de aplicación es ejecutado por el software básico y proporciona los procedimientos de aplicación y las interfaces de usuario para el funcionamiento del

CliniMACS Prodigy en función de su uso previsto:

- como parte del sistema de separación de células CliniMACS Prodigy para separar células humanas
- como parte del sistema CliniMACS Prodigy de fabricación de células y terapia génica para la manipulación genética u otras manipulaciones sustanciales (como la proliferación, la diferenciación) de las células humanas.

El software básico y cada aplicación son elementos independientes que permiten actualizar por separado una nueva aplicación sin cambiar el software básico.

1.2 Información regulatoria

El software ha sido desarrollado de acuerdo con la norma IEC/EN 62304. Además, el software básico del CliniMACS Prodigy se ha desarrollado para cumplir con GAMP 5, EudraLex Volumen 4 Anexo 11 (EU GMP Anexo 11) y 21 CFR Parte 11.

Los requisitos de ciberseguridad se cumplen de acuerdo con la norma IEC 81001-5-1, incluidas las pruebas de penetración realizadas por una tercera empresa.

La descripción general completa de la información regulatoria, incluido el uso previsto, figura en el manual del usuario del instrumento CliniMACS Prodigy.

1.3 Normativas de protección de datos

Al procesar datos personales con el sistema CliniMACS Prodigy, se recomienda encarecidamente la discreción del usuario. El usuario es responsable de garantizar el cumplimiento de las normativas y los reglamentos de protección de datos aplicables. De acuerdo con los principios de privacidad por diseño y por defecto, Miltenyi ha introducido medidas de seguridad, especialmente el concepto de defensa en profundidad (ver la sección 4.1 ´Concepto de defensa en profundidad para la seguridad´).

1.4 Acerca de este manual

Este manual del usuario proporciona la información necesaria para la configuración y el funcionamiento seguro del software básico. En este manual solo se incluye el software básico 2.2.

1.5 Documentos relacionados

El manual del usuario del instrumento CliniMACS Prodigy describe el hardware y el sistema del instrumento CliniMACS Prodigy. El manual del usuario del instrumento se suministra junto con el presente manual.

El manual del usuario del instrumento incluye:

- Advertencias, precauciones, notas
- Información regulatoria
- Datos técnicos
- Otra información importante

Si utiliza el CliniMACS Prodigy junto con el MACS® TubeSealer, el CliniMACS Electroporator, la CliniMACS Formulation Unit o el CliniMACS Workbench, tenga en cuenta los siguientes manuales del usuario asociados:

- Manual del usuario del MACS TubeSealer
- Manual del usuario del CliniMACS Electroporator
- Manual del usuario de la CliniMACS Formulation Unit
- Manual del usuario del CliniMACS Workbench

En el manual del usuario del instrumento CliniMACS Prodigy encontrará un resumen completo de los accesorios, componentes e instrumentos MACS GMP disponibles.

Para obtener información sobre aplicaciones específicas, póngase en contacto con Miltenyi Biotec Technical Support.

2
Glosario

2.1 Nivel de peligro

El color y la palabra de advertencia de un mensaje de advertencia dependen del nivel de peligro. El nivel de peligro clasifica el peligro según se describe a continuación. El tipo, nivel y origen del peligro, así como sus posibles consecuencias, prohibiciones y medidas, se indican del siguiente modo.

⚠ ADVERTENCIA

Indica una situación peligrosa que, si no se evita, puede provocar la muerte o lesiones graves.

⚠ ATENCIÓN

Indica una situación peligrosa que, si no se evita, puede provocar lesiones leves o moderadas.

AVISO

Indica información que se considera importante, pero no relacionada con el peligro (p. ej., mensajes relacionados con daños materiales).

IMPORTANTE

Advierte al usuario de prácticas o informaciones importantes no relacionadas con daños personales ni materiales.

2.2 Convenciones de estilo y formato

El texto en **<verde claro>** indica elementos de la interfaz gráfica de usuario (p. ej., botones, cuadros de diálogo o elementos de administración de usuarios).

2.3 Glosario de símbolos y términos

En el manual del usuario del instrumento CliniMACS Prodigy se ofrece un resumen de los símbolos y términos generales utilizados en el sistema CliniMACS Prodigy. El glosario de símbolos muestra los símbolos utilizados para el etiquetado de los productos CliniMACS.

2.3.1 Términos específicos del software

Proceso de aplicación	Software para el procesamiento celular desarrollado por Miltenyi Biotec.
ATS Aaudit Trail System	Un componente de software que rastrea y registra los sucesos, las acciones, entradas de usuario y los cambios realizados en el software CliniMACS Prodigy.
CAP	Proceso de aplicación personalizada (Customized Application Process)
FTP File Transfer Protocol	Protocolo de comunicación estándar utilizado para la transferencia de archivos informáticos de un servidor a un cliente en una red informática.
LDAP Lightweight Directory Access Protocol	Protocolo de aplicación para acceder y mantener los servicios de información de directorio distribuidos a través de una red de protocolo de Internet.
MD5	Algoritmo utilizado para crear la suma de comprobación y verificar la integridad de los datos frente a la corrupción involuntaria.

SMB Server Message Block	Protocolo de comunicación utilizado para compartir archivos, impresoras, puertos serie y diversas comunicaciones entre nodos de una red.
SMTP Simple Mail Transfer Protocol	Protocolo de comunicación para la transmisión de correo electrónico.
Proceso de aplicación estándar	Un proceso de aplicación prevalidado por Miltenyi Biotec.
UMS User Management System	Un componente de software para administrar y controlar el acceso de los usuarios a las distintas funciones del instrumento.

3

Informaciones de seguridad importantes

3.1 Instrucciones de seguridad para el CliniMACS Prodigy

Para información detallada sobre la seguridad del instrumento, consultar el manual del usuario del instrumento del CliniMACS Prodigy.

3.2 Instrucciones de seguridad del software

IMPORTANTE

Antes del uso se debe validar el control de acceso del instrumento. No divulgar el nombre de usuario ni la contraseña. Se recomienda establecer una solución de emergencia (ver el capítulo 10 ´Administración de usuarios´). Si fallara el inicio de sesión durante la ejecución de un proceso, póngase en contacto con Miltenyi Biotec Technical Support.

- Antes de utilizar el instrumento con la versión de software 2.2, leer el capítulo 3 «Información de seguridad importante» del manual del usuario del instrumento del CliniMACS Prodigy y toda la demás información contenida en este manual del usuario del software, incluidas las instrucciones de seguridad y funcionamiento.
- Prestar especial atención a todas las advertencias que aparecen en el instrumento.
- Si no se leen y siguen estas pautas, podría utilizarse de forma inadecuada o incorrecta y podrían producirse daños en el instrumento. El uso inadecuado también puede causar graves lesiones personales, muerte, resultados impredecibles, mal funcionamiento del instrumento y un desgaste prematuro de los componentes que acortara la vida útil del instrumento. Estas acciones pueden anular su garantía.
- Para consultas futuras, mantenga en un lugar seguro y accesible para todos los usuarios el manual del usuario y cualquier otra instrucción de manejo y seguridad suministrada con el instrumento.
- Todos los procedimientos de procesamiento solo los deben realizar los usuarios debidamente formados. El usuario debe tener una comprensión general del procesamiento celular y conocimientos sobre bioseguridad.
- La instalación, el mantenimiento y el servicio técnico del instrumento los debe realizar exclusivamente un proveedor de servicios autorizado de Miltenyi Biotec.
- La comunicación y el acceso a los datos entre el software y el servidor/aplicación externos se deben validar antes del uso.
- En caso de duda sobre el uso seguro del instrumento, póngase en contacto con Miltenyi Biotec Technical Support.
- En caso de problemas o fallos, póngase en contacto con Miltenyi Biotec Technical Support.

4

Ciberseguridad

4.1 Concepto de defensa en profundidad para la seguridad

La ciberseguridad es una responsabilidad compartida entre Miltenyi Biotech y los usuarios. El software está diseñado con medidas de seguridad integradas para ofrecer protección contra las amenazas más comunes. Los usuarios deben desempeñar un papel activo en la protección de los datos y en el mantenimiento de prácticas seguras. En consonancia con el uso previsto, se recomienda un modelo de defensa en profundidad. Los objetivos de este modelo de defensa en profundidad son:

- Evitar repercusiones negativas en la calidad y el retraso del producto celular
- Mantener la integridad de los protocolos, procesos y datos de auditoría
- Mantener la integridad de la configuración del aparato
- Garantizar la disponibilidad del instrumento para el procesamiento celular
- Permitir el acceso únicamente a usuarios formados y autorizados

El modelo de defensa en profundidad se estructura en las siguientes capas:

- Capa de protección física
- Capa de entorno de red
- Capa de software del instrumento
- Capa de usuario
- Capa de auditoría
- Capa de gestión de actualizaciones
- Capa de gestión de vulnerabilidades
- Capa de copia de seguridad y recuperación

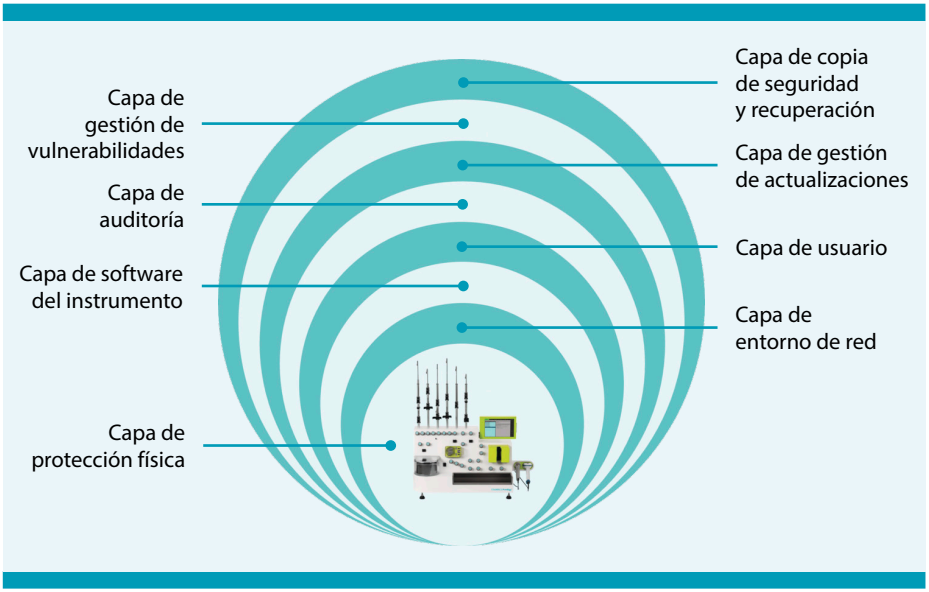


Figura 4.1: Capas del concepto de defensa en profundidad

4.1.1 Capa de protección física

El instrumento dispone de las siguientes interfaces físicas que permiten conectar los distintos componentes, accesorios e instrumentos (ver la Tabla 4.1). El cliente es responsable de garantizar que únicamente personal autorizado tenga acceso físico al producto y de proporcionar procesos adecuados para controlar y supervisar el acceso físico.

Interfaz	Propósito
Puerto USB	Conectar al instrumento periféricos homologados, como el teclado externo o el lector de códigos de barras. Se puede utilizar un conector USB-Ethernet para conectar el instrumento a la red informática. Se pueden utilizar memorias USB flash para transferir protocolos, imágenes y archivos de registro desde el instrumento y transferir programas/actualizaciones al instrumento, así como para la instalación del instrumento.
Pantalla táctil	Dispositivo de introducción de datos utilizado por el personal de mantenimiento y servicio, así como por los operarios.
CAN bus/alimentación eléctrica Interfaz CAN	La interfaz permite la conexión del instrumento a dispositivos adicionales, como el CliniMACS Electroporator o la CliniMACS Formulation Unit.
Conector para el sellador de tubos	Proporciona alimentación eléctrica al MACS TubeSealer, un sellador térmico instalado en el CliniMACS Prodigy. No se trata de una interfaz de datos.
Conector de alarma	Conector del circuito de relés para la conexión del instrumento a un sistema de alarma externo. No se trata de una interfaz de datos.

Tabla 4.1: Interfaces y periféricos del instrumento

Los puertos USB permiten conectar memorias USB flash. Aunque existen medidas del sistema operativo y de la aplicación para gestionar las conexiones USB, es responsabilidad del cliente asegurarse de que solo se utilicen con el instrumento memorias USB flash aprobadas y controladas.

Nota: Solo se admiten unidades USB flash con formato FAT32. Una manipulación inadecuada (p. ej., uso de fuerza física) de las interfaces o de los accesorios puede dañar las interfaces físicas del instrumento y dejarlas inoperativas, lo que entraña un riesgo residual.

4.1.2 Capa de entorno de red

El instrumento se debe utilizar en un segmento de red protegido separado de otros segmentos. Se muestra una posible configuración en la que el instrumento forma parte de una red de instrumentos aislada en Figura 4.2. Un enrutador separa los distintos segmentos de la red entre sí y controla el flujo de datos entre ellos.

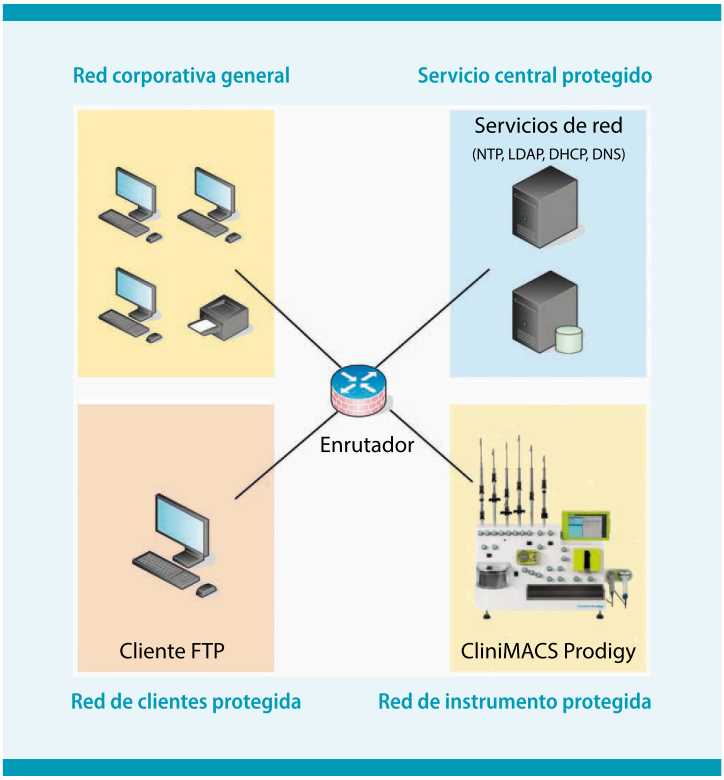


Figura 4.2: Diagrama de red

El instrumento ofrece principalmente funciones para establecer conexión con otros sistemas de la red. Los protocolos de red compatibles se enumeran en la Tabla 4.2.

Interfaz	Propósito	Puerto	Comentario
FTP	Acceso de solo lectura al archivo de registro a través de FTP	20 – 21	El uso de FTP permite transmitir los archivos de registro y las contraseñas en texto no cifrado a través de la red. Se recomienda utilizar una cuenta de usuario específica para acceder a los datos a través de FTP a fin de limitar el riesgo para el servicio FTP y evitar el movimiento lateral en caso de que se vea comprometida la cuenta de usuario. FTP está desactivado por defecto.
NTP	Sincronización de la hora	123	–
DNS (cliente)	Resuelve los nombres de host a direcciones IP	53 (UDP)	–
Solicitud/ respuesta de eco ICMP (servidor)	Permite comprobar la conexión de red con el instrumento	N/A	–
DHCP (cliente)	La configuración de red automática del instrumento	68 (UDP)	–
LDAP	Permite iniciar sesión en el instrumento con las credenciales de Active Directory que se gestionan de forma centralizada	389	Protocolo no seguro, solo se debe utilizar si no se admite LDAPS
LDAPS	Versión segura de LDAP	636	Una variante segura de LDAP. Requiere una configuración adecuada, ver la sección 9.2 «Conexión a un servidor LDAP».
SMB	Intercambio de archivos	445	Se admite el intercambio autenticado. Requiere configuración, ver la sección 9.3 «Conexión a una unidad de red»
SMTP	Notificación por correo electrónico	25, 2525, 465, 587	Se admite autenticación, requiere una configuración adecuada, ver la sección 9.5 «Conexión a un servidor de correo electrónico»
SMTPS	Versión segura de SMTP	465, 587	Una variante segura de SMTP. Requiere una configuración adecuada, ver la sección 9.5 ´Conexión a un servidor de correo electrónico´

Tabla 4.2: Conexiones y protocolos de red

IMPORTANTE

Excepto para FTP, se admiten protocolos seguros para todos los servicios. Se recomienda encarecidamente activar solo las funciones seguras enumeradas en la Table 4.2. Por razones de compatibilidad, se admiten versiones inseguras de los protocolos. En los casos en los que el protocolo inseguro sea necesario por razones de compatibilidad, el cliente deberá aplicar las medidas de mitigación adecuadas.

El cliente es responsable de garantizar que únicamente personal autorizado tenga acceso de red al instrumento y a las redes utilizadas para transferir los protocolos activados. Se deben haber implementado procesos adecuados para controlar y supervisar el acceso a la red. Además, el instrumento no debe estar expuesto directamente a Internet.

4.1.3 Capa de software del instrumento

En el instrumento se utiliza un sistema operativo Linux personalizado. Solo se habilitan el software, los servicios y las funciones del núcleo necesarios para minimizar la superficie de ataque del software del instrumento.

El acceso a la BIOS de los PC del instrumento solo está disponible para el personal de servicio formado por Miltenyi. La configuración de la BIOS impide el arranque desde medios externos para garantizar la integridad del software del instrumento.

Se han adoptado medidas para garantizar que en el instrumento solo se pueda ejecutar software autorizado. El nuevo software se instala en el instrumento por medio de una memoria USB flash. No es posible realizar un inicio automático del software desde la memoria USB flash y los operarios no podrán iniciar aplicaciones directamente desde una memoria USB flash.

El software adicional (que generalmente deberá estar disponible en el instrumento) se debe instalar mediante un instalador suministrado con este software. Para garantizar que solo se pueda instalar el software original de Miltenyi Biotec previsto para el instrumento, se realizan varias comprobaciones. Más concretamente, el instalador comprueba la fecha de caducidad del paquete de instalación y la firma electrónica del software que se va a instalar en el instrumento. Si fallara una comprobación, el software no se podrá instalar. Antes de ejecutar la instalación, es necesario «inyectar» el paquete de software, es decir, copiarlo en la memoria volátil del instrumento mediante la herramienta Custom Files. Esta herramienta garantiza que, además de los formatos ejecutables exclusivos, solo se puedan copiar en el instrumento los archivos originales firmados por Miltenyi Biotec para su ejecución.

La instalación de una nueva versión del software del instrumento se describe abajo, en la sección 4.1.6 ´Capa de gestión de actualizaciones´.

Las nuevas versiones del software del instrumento o del software de aplicación personalizado las instalará el Miltenyi Biotec Technical Support.

En el sistema no se ejecuta ningún otro software de detección de malware, ya que no es adecuado para este producto. En cambio, el riesgo de malware se controla por medio de este concepto de defensa en profundidad.

El software de aplicación y las herramientas validan la verosimilitud de las entradas de los usuarios. Esta validación incluye, entre otras cosas, la validación de intervalos para entradas numéricas, la validación de los números de lote y de producto de los consumibles y la comprobación de la verosimilitud de las entradas.

El software y las aplicaciones no solicitan durante su ejecución que se facilite información sanitaria personal, por lo que el riesgo de que el operario la introducir durante la ejecución de la aplicación es bajo. Es responsabilidad del usuario garantizar el cumplimiento de la normativa aplicable en materia de privacidad.

Los protocolos y los datos de registro se pueden exportar desde el instrumento. Los datos exportados van acompañados de «hashes» de archivo para que el operario pueda comprobar que la exportación y la transferencia a un sistema posterior se hayan realizado correctamente y que no se haya producido ninguna corrupción de datos relacionada con la transferencia. Actualmente, el algoritmo utilizado es MD5.

El acceso al software destinado a fines de mantenimiento y a la funcionalidad restringida de los procedimientos de aplicación solo está disponible para el Miltenyi Biotec Technical Support y no para el cliente en operaciones normales. El acceso está disponible para los usuarios que inicien sesión con la cuenta de servicio o con una memoria USB flash de servicio, es decir, una memoria USB flash con información de autenticación y el PIN asociado, o a través de la funcionalidad de acceso remoto de la herramienta Info, en combinación con un PIN de un solo uso proporcionado por Miltenyi Biotec. Solo el Miltenyi Biotec Technical Support tiene acceso a las credenciales de la cuenta de servicio y a la memoria USB flash de servicio. El servicio de asistencia técnica puede proporcionar un PIN de un solo uso durante los casos de asistencia remota.

IMPORTANTE

No se ha implementado ninguna protección para evitar que se lean o manipulen intencionadamente los datos exportados. El cliente deberá asegurarse de que solo personal autorizado tenga acceso a los datos exportados.

4.1.4 Capa de usuario

Todos los accesos al componente se pueden proteger mediante una administración de usuarios configurable. El cliente deberá asegurarse de que se apliquen las instrucciones y recomendaciones que figuran en este documento.

Además, el cliente deberá asegurarse de que solo personal formado y autorizado tenga acceso al instrumento y de que se sigan las mejores prácticas comunes en cuanto al uso de contraseñas y la normativa aplicable.

4.1.5 Capa de auditoría

El sistema de audit trail registra información sobre las acciones realizadas en el instrumento, p. ej., entradas del operario durante la ejecución de una aplicación o cambios en la configuración del instrumento. Si está activada el audit trail, las acciones se registrarán en el audit trail del instrumento. El cliente debe asegurarse de que se observen las instrucciones y recomendaciones que figuran en este documento.

Aunque los datos del audit trail los genera el instrumento, el manejo inadecuado de los datos del audit trail constituye un riesgo residual. Para mitigar el riesgo, el cliente es responsable de la seguridad y el tratamiento de los datos del audit trail (p. ej., exportación, almacenamiento, eliminación y revisión) de acuerdo con la normativa aplicable.

4.1.6 Capa de gestión de actualizaciones

Las actualizaciones de seguridad se envían en el contexto de paquetes de actualización. Miltenyi Biotec informará al cliente cuando esté disponible un nuevo software.

Las actualizaciones del software del instrumento las debe realizar únicamente el Miltenyi Biotec Technical Support. Las actualizaciones del software del instrumento se suministran e instalan según los procedimientos descritos en los PNT de Miltenyi Biotec. Las actualizaciones se empaquetan en paquetes específicos que contienen el nuevo software del instrumento, así como el software que realiza la instalación propiamente dicha. Las actualizaciones se suministran en una memoria USB flash. Para garantizar la integridad del paquete, todos los componentes están firmados criptográficamente, lo que se comprueba antes de la instalación. Póngase en contacto con Miltenyi Biotec Technical Support para programar una actualización del instrumento.

4.1.7 Capa de gestión de vulnerabilidades

Para notificar una vulnerabilidad de seguridad o un incidente que afecte al producto o a uno de sus componentes, póngase en contacto con Miltenyi Biotec Technical Support (ver el capítulo 11 ´Resolución de problemas´).

4.1.8 Capa de copia de seguridad y recuperación

El instrumento solo ofrece la funcionalidad para realizar copias de seguridad de protocolos y datos. El cliente deberá asegurarse de que se realice periódicamente una copia de seguridad de esos datos y de que esta cumpla la normativa aplicable. Si el software del instrumento deja de funcionar, póngase en contacto con Miltenyi Biotec Technical Support.

4.1.9 Resumen de la configuración segura

En las secciones anteriores se han presentado las medidas de seguridad implementadas y se recomiendan las medidas que se deberán aplicar para el funcionamiento seguro del CliniMACS Prodigy. Estas medidas se incluyen en los ámbitos de configuración del instrumento, de los procedimientos y las políticas que aumentan la seguridad del instrumento. Se recomiendan las siguientes medidas:

- Asegurarse de que solo el personal autorizado tenga acceso físico al instrumento y a sus interfaces físicas.
- Asegurarse de que el acceso a la red en la que se utilice el instrumento esté limitado al personal y los sistemas autorizados.
- Activar la autenticación y autorización en cada instrumento para garantizar que solo el personal autorizado pueda acceder al software del instrumento.
- El cliente debe disponer de una gestión de autorizaciones adecuada para garantizar que al personal que utilice o acceda al instrumento solo se asignen los derechos necesarios para ejecutar la función de la tarea (principio de privilegio mínimo).
- Configurar una política de contraseñas adecuada para seguir las mejores prácticas y cumplir la normativa aplicable.
- Si el instrumento los admite, se deberá dar preferencia a los protocolos seguros frente a las variantes inseguras.
- Debido a la falta de encriptación del tráfico FTP hacia y desde el instrumento, se recomienda configurar y utilizar un usuario específico para acceder a los datos a través de FTP.
- Se deberán establecer procesos y procedimientos para garantizar que solo se utilicen memorias USB flash autorizadas y controladas e impedir el uso de otras memorias USB flash.
- Se deberán establecer procesos y procedimientos que garanticen el tratamiento adecuado del audit trail, los protocolos y los datos de registro de acuerdo con la normativa aplicable.
- El personal debe recibir formación sobre concienciación en materia de seguridad e higiene básica de seguridad.
- Los procesos y procedimientos deben garantizar que las copias de seguridad del instrumento se realicen periódicamente y sigan la normativa aplicable.
- El cliente es responsable de que no se utilice información sanitaria personal en el instrumento.

5
Concepto de software

5.1 Concepto básico

El software que se ejecuta en el instrumento se compone del software básico y de diversos programas de aplicación (denominados «proceso de aplicación»). El software básico proporciona una plataforma común para todos los programas ejecutables, incluidos los procesos de aplicación, las herramientas y los ajustes.

Proceso de aplicación

Un software independiente representa un proceso biológico, p. ej., Proceso de transducción de linfocitos T o LP-34 Enrichment. Contiene una secuencia de pasos predefinidos de hardware y software para automatizar el proceso biológico. Durante el proceso, se guiará al usuario paso a paso. Hay dos tipos de procesos de aplicación:

- Proceso de aplicación estándar: un proceso de aplicación prevalidado proporcionado por defecto.
- Proceso de aplicación personalizada (CAP): un proceso de aplicación a medida diseñado para clientes especializados.

Herramienta

Programa ejecutable que puede ejecutar una función de propósito general fuera de un proceso de aplicación. Por ejemplo, comprobar o cambiar el estado del hardware, transferir datos, apagar el instrumento, etc.

Ajuste

Un programa ejecutable para configurar el instrumento. Por ejemplo, Network Settings (Ajustes de red), Customer Settings (Ajustes personalizados) y Module Settings (Ajustes del módulo).

Para cada programa ejecutable se creará una carpeta que contendrá toda la información. El nombre de la carpeta está compuesto por [Fecha] _ [Hora] _ [Número de serie] _ [Programa ejecutable].

El contenido de esta carpeta lo controla el programa ejecutado. En los procesos de aplicación, los archivos relevantes para el cliente se enumeran en la Tabla 5.1.

Nombre de archivo/carpeta	Descripción	Formato
Protocol.pdf	Registro electrónico de la ejecución de la aplicación	.pdf
Prototol_ Appendix_I.pdf	Registro de errores y advertencias durante la ejecución de la aplicación	.pdf
Interphase	Imágenes de cámara intercapas	Carpeta
Microscope	Imágenes microscópicas adquiridas durante la aplicación	Carpeta
checksums.md5	Suma de comprobación	.md5
IR_Monitor	Registra la hora y la temperatura si la temperatura de la superficie de la cámara está fuera de especificación durante el cultivo celular	.html

Tabla 5.1: Archivos de registro de los procesos de aplicación

5.2 La interfaz gráfica de usuario

La interfaz gráfica de usuario (GUI) contiene varias secciones: barra de menús (con menú de acceso rápido), barra de herramientas, línea de estado y área de contenidos (Figura 5.1).Durante el funcionamiento del software, los elementos y el contenido de la interfaz gráfica de usuario cambian en función de la actividad y el proceso.

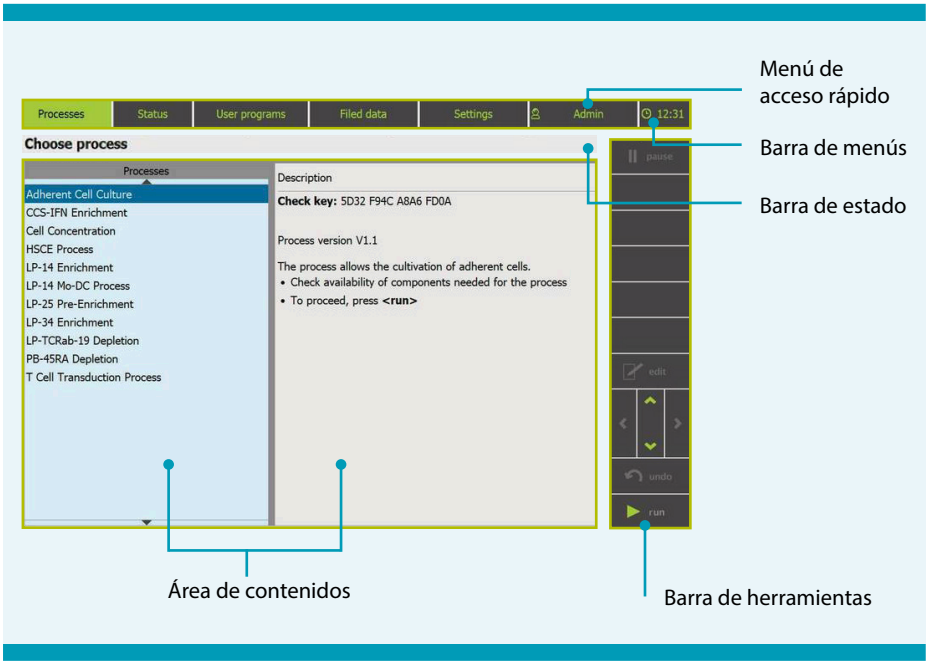


Figura 5.1: Secciones de la interfaz gráfica de usuario

5.2.1 Barra de menú y área de contenidos

La barra de menú proporciona acceso a **<Processes>** (Procesos), **<Status>** (Estado), **<User Programs>** (Programas), **<Filed data>** (Archivos), **<Settings>** (Ajustes) y (menú de acceso rápido) (quick access menu). Un fondo verde indica qué botón de menú está activo. Tocar en el área respectiva para activar el menú. El área de contenidos se adapta según el menú seleccionado. Al iniciar sesión, **<Processes>** se selecciona de forma predeterminada y se muestra el contenido de los procesos (ver la Figura 5.1).

Menú	Descripción
<Processes> (Procesos)	Acceso a los procesos de aplicación estándar instalados en los instrumentos (Pantalla 6.5) y guía a través de la ejecución del proceso (Pantalla 6.6)
<Status> (Estado)	Estado del instrumento durante la ejecución de un proceso de aplicación (Figura 6.1)
<User Programs> (Programas)	Acceso al proceso de aplicación personalizada (CAP) de Miltenyi Biotec y guías para la ejecución del proceso
<Filed data> (Archivos)	Acceso a la visualización y exportación de datos generados por procesos, herramientas y ajustes (Pantalla 7.1).
<Settings> (Ajustes)	Acceso a ajustes y herramientas para la configuración de instrumentos, pruebas de funcionamiento y resolución de problemas básicos (Pantalla 8.1)
Quick access menu (Menú de acceso rápido)	Acceso al cierre de sesión, a la administración de usuarios, la política de contraseñas, el audit trail y el botón de apagado (Pantalla 6.3)
System time (Hora del sistema)	Hora actual del sistema.

Tabla 5.2: Menús en la barra de menús

5.2.2 Barra de estado

La línea de estado (ver la Figura 5.1) contiene información resumida referente al estado del proceso actual.

5.2.3 Barra de herramientas

La barra de herramientas contiene diferentes botones para controlar el proceso. La disponibilidad de los botones y su estado activo se controlan por medio del proceso de aplicación. La Figura 5.2 muestra ejemplos de barras de herramientas durante dos procesos de aplicación diferentes. Un color verde indica un estado «activo», y un color gris un estado «inactivo».
Los botones de uso frecuente se explican en la Tabla 5.3.

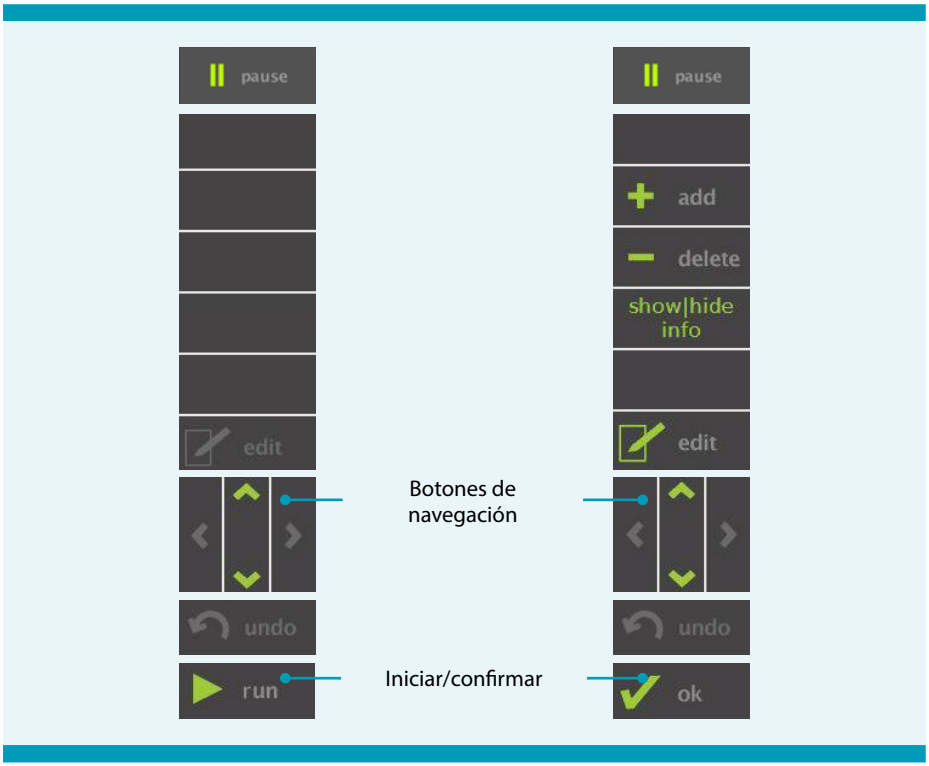


Figura 5.2: Botones dinámicos y estáticos de la barra de herramientas

Nombre del botón	Descripción	Disponibilidad
<pause>	permite parar/suspender temporalmente el proceso en curso, depende de la aplicación en curso	durante la ejecución de un proceso
<edit>	permite activar el campo de entrada para introducir datos manualmente (ver 5.2.4 ´Campos de entrada´).	si los campos de entrada están disponibles
botones de navegación	permiten seleccionar elementos de una lista: use ^v para desplazar el elemento seleccionado hacia arriba o hacia abajo en la lista (ver la Pantalla 6.5) o < > para cambiar entre listas (ver la Pantalla 8.1). permite navegar por las imágenes de la cámara (Figura 6.3).	siempre si la cámara está activa
<undo>	permite revocar una o varias entradas para restablecer el contenido original de la pantalla	durante la ejecución de un proceso
<ok>/<run>	<ok> confirma una selección o cierra el menú activo <run> inicia un proceso, un programa de usuario o cualquier otro procedimiento	siempre

Tabla 5.3: Botones de uso frecuente en la barra de herramientas

5.2.4 Campos de entrada

Un campo de entrada representa un teclado y permite introducir letras o números (ver la Figura 5.3). Para introducir letras mayúsculas manualmente, tocar <⇧>, para espacio tocar <SP>, para números tocar <?123> y para retroceso tocar <⌫>. Para abrir los campos de entrada, tocar <editar> en la barra de herramientas. Para cerrar el campo de entrada, tocar <ok> en la parte inferior de los campos de entrada para confirmar la entrada o tocar <Escape> en la parte superior derecha para cerrar sin guardar.

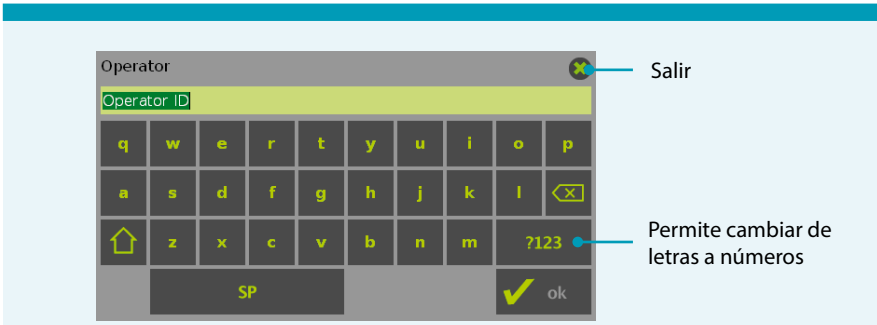
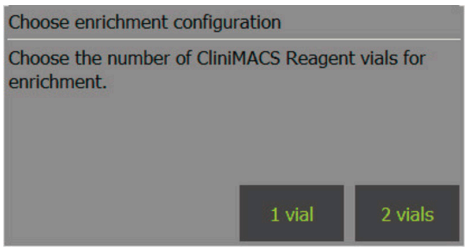


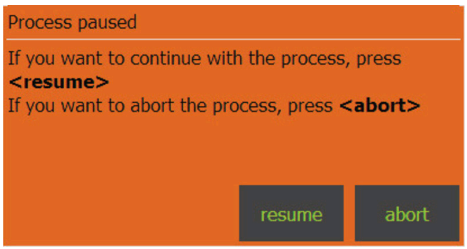
Figura 5.3: El campo de entrada – teclado con letras

5.2.5 Ventanas emergentes

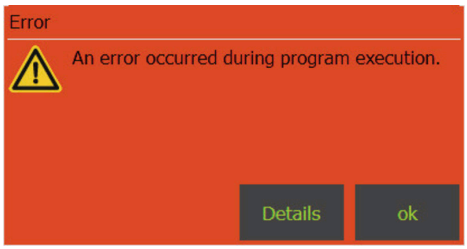
Al ejecutar programas ejecutables pueden aparecer ventanas emergentes. El proceso en curso se interrumpirá hasta que se cierre la ventana emergente. En caso necesario, las ventanas emergentes se pueden arrastrar por la pantalla manteniendo pulsada la barra superior. Hay varias situaciones en las que se mostrará una ventana emergente:



Se requiere entrada o confirmación. La ventana emergente muestra un fondo gris. Seleccionar uno de los botones para continuar con el proceso.



Se debe confirmar una advertencia del instrumento o una decisión importante. La ventana emergente muestra un fondo naranja. Para tomar una decisión, seleccionar uno de los botones.



Se ha producido un error. La ventana emergente muestra un fondo rojo. Seleccionar uno de los botones de la parte inferior para continuar.

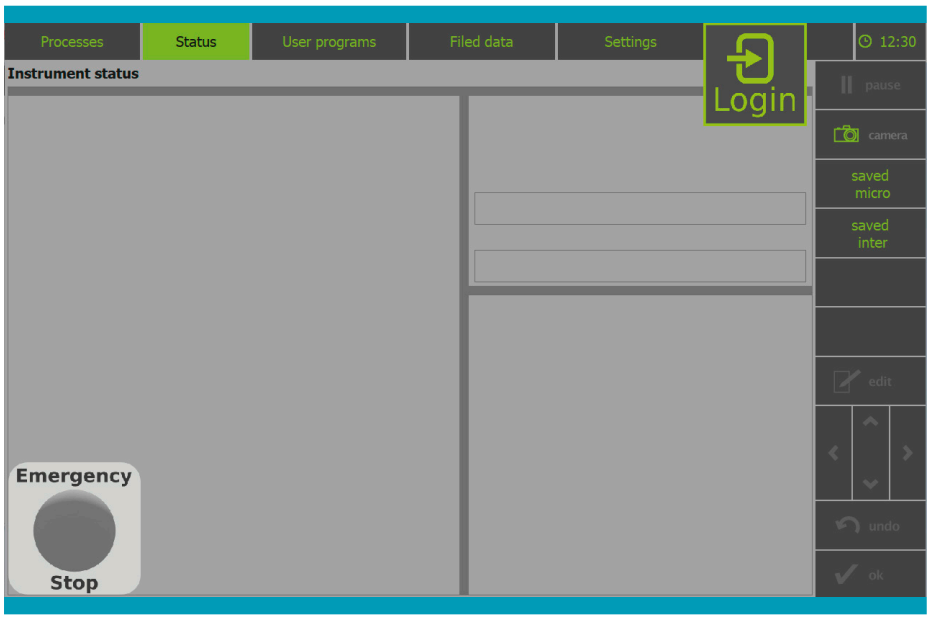
En caso necesario, póngase en contacto con Miltenyi Biotec Technical Support

6

Manejo básico

6.1 Encendido del instrumento

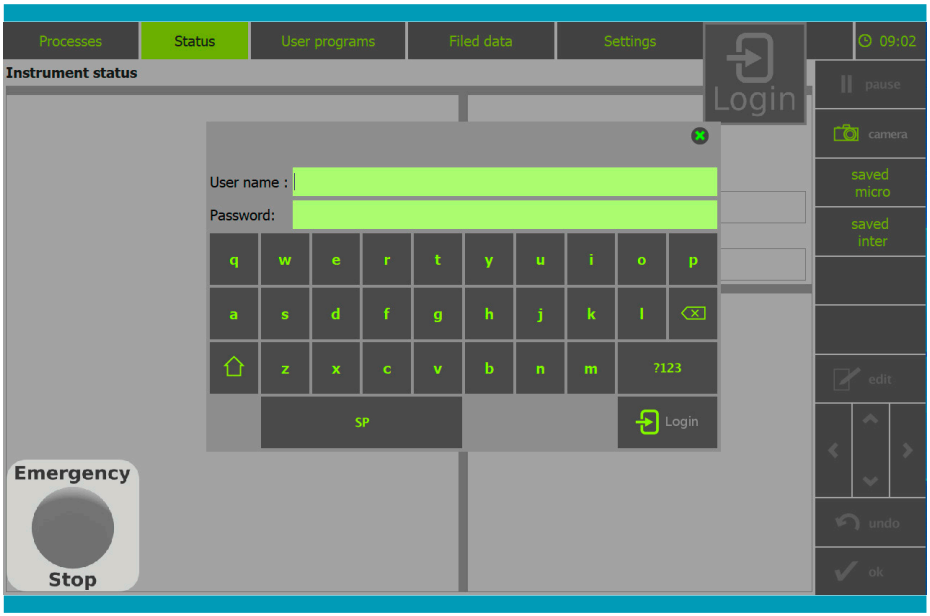
Encienda el CliniMACS Prodigy con el interruptor de encendido/apagado situado en el lado posterior del instrumento. La pantalla de inicio mostrará la versión del software y aparecerá el proceso de inicialización durante un breve espacio de tiempo (aprox. 5 segundos). Tras el proceso de inicialización, aparecerá una pantalla bloqueada (ver la Pantalla 6.1). En esta pantalla solo está activado el botón <Login>.



Pantalla 6.1: Pantalla bloqueada

6.2 Inicio de sesión

Tocar <Login> en la esquina superior derecha de la pantalla para abrir la ventana emergente <User Login> (ver la Pantalla 6.2). Introducir el nombre de usuario y la contraseña y tocar <Login> en la ventana emergente. La pantalla se desbloqueará. Antes del uso, se deben configurar el nombre de usuario y la contraseña (ver el capítulo 10 ´Administración de usuarios´ para más detalles).



Pantalla 6.2: Ventana de inicio de sesión del usuario

Nota: Si fallara el inicio de sesión, póngase en contacto con un administrador del sistema para verificar:

- si el nombre de usuario y la contraseña son correctos.
- los derechos de acceso de esta cuenta. Para más información, consultar el capítulo 10 «Administración de usuarios»).

Si aparece una notificación emergente durante el inicio de sesión no relacionada con credenciales del usuario incorrectas ni con derechos de acceso insuficientes, tocar <ok>. A continuación, introducir de nuevo las credenciales del usuario.

Si sigue fallando el inicio de sesión, ponerse en contacto con Miltenyi Biotec Technical Support.

6.3 Cierre de sesión

Tocar (menú de acceso rápido) y seleccionar en la lista <Logout> (ver la Pantalla 6.3). La pantalla se volverá a bloquear.

Nota: Transcurridos 20 minutos sin interacción con el software, la sesión del usuario se cerrará automáticamente.



Pantalla 6.3: Cierre de sesión

6.4 Apagado

Tocar (menú de acceso rápido). Seleccionar en la lista <Shutdown> (ver la Pantalla 6.3). También puede ir a <Settings> ▸ <Tools> ▸ <Shutdown>. Esperar a que finalice el proceso de apagado y, a continuación, apagar el instrumento con el interruptor de encendido/apagado situado en la parte posterior.

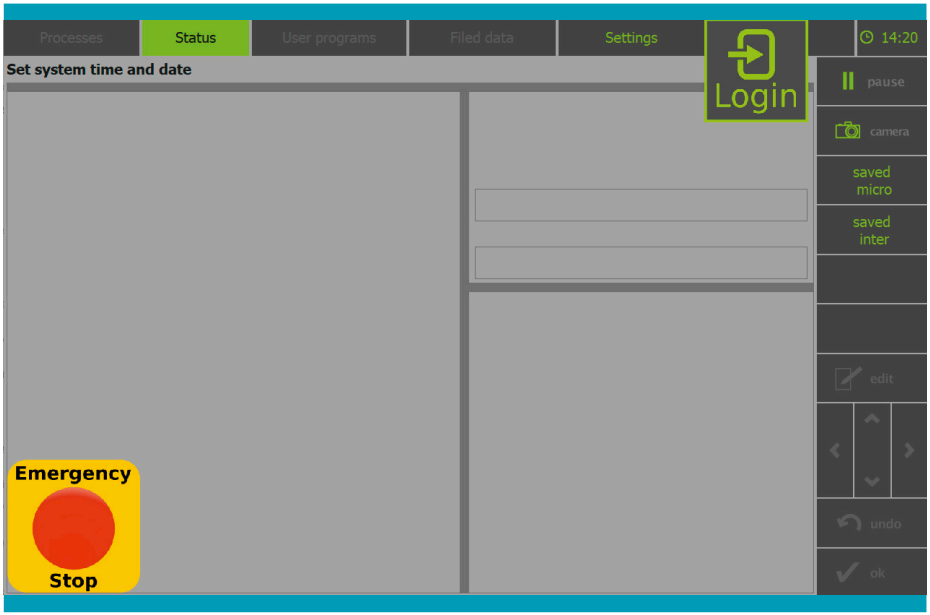
6.5 Parada de emergencia

<Emergency Stop> pausa la aplicación en curso o una herramienta en caso de una situación de emergencia sin necesidad de iniciar sesión previamente. Para cumplir los requisitos de 21 CFR Parte 11, es necesario iniciar sesión posteriormente e introducir el motivo de la parada de emergencia. El botón <Emergency Stop> solo se activará (lo que se indica con los colores amarillo y rojo) si se está ejecutando una aplicación o una herramienta y ningún usuario ha iniciado sesión (ver la Pantalla 6.4).

IMPORTANTE

El botón de parada de emergencia <**Emergency Stop**> no apaga completamente el instrumento, pero tiene la misma función que el botón <**pause**> durante una aplicación activa cuando un usuario está conectado.

Para reanudar la aplicación, deberá iniciar sesión el usuario con los derechos correspondientes para la aplicación.

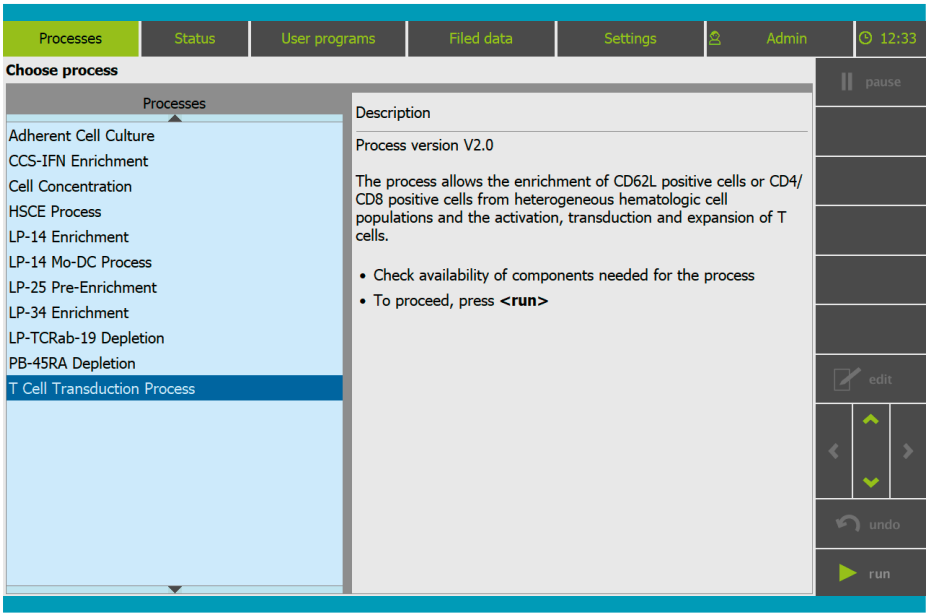


Pantalla 6.4: Botón de parada de emergencia

6.6 Seleccionar un proceso de aplicación

1. Tocar <**Processes**> en la barra de menús para ejecutar un proceso de aplicación estándar. Para una CAP, tocar <**User Programs**>.
2. Seleccionar el proceso deseado de la lista de procesos(Pantalla 6.5). El proceso seleccionado se resalta con fondo azul. La descripción de la aplicación figura a la derecha. Tocar en la lista de procesos o utilice ^ y ˇ de la barra de herramientas para desplazarse por los procesos disponibles.

Nota: El contenido de la lista de procesos se adapta a la función y los derechos del usuario actual. Solo se mostrará una aplicación si el usuario que ha iniciado actualmente sesión tiene derechos de acceso. Para más información relativa a funciones y derechos, ver el capítulo 10 ´Administración de usuarios´.



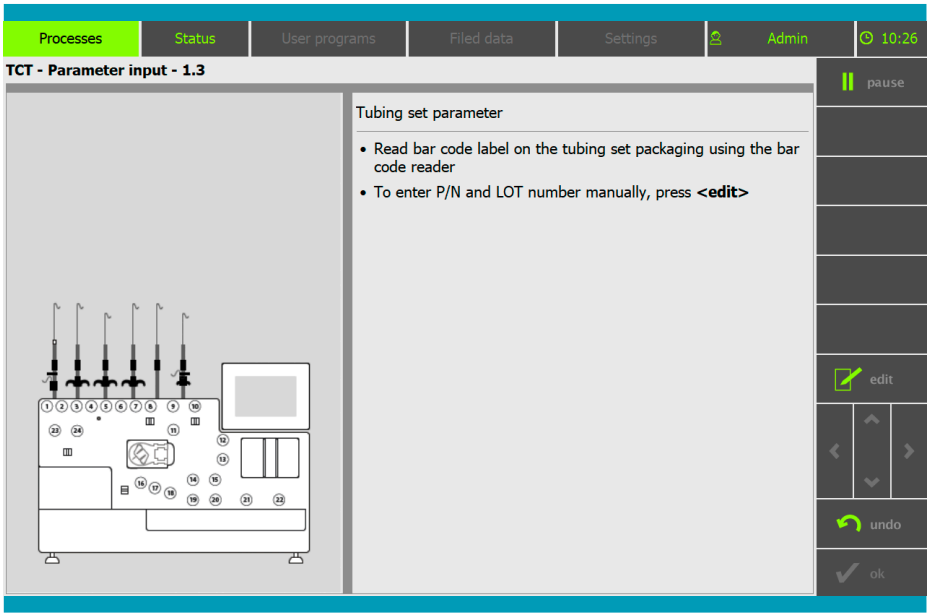
Pantalla 6.5: Selección de un proceso de aplicación

6.7 Ejecutar un proceso de aplicación

Para iniciar el proceso, seleccionarlo y tocar **<run>** en la barra de herramientas. El programa le guiará paso a paso por el proceso.
Pantalla 6.6 muestra un paso de ejemplo de la aplicación TCT. La línea de estado muestra el nombre y el índice del paso actual. El área de contenidos proporciona más información sobre el paso correspondiente. Seguir la ilustración y las instrucciones del área de contenidos para cada paso.

En determinados pasos del procesamiento se requiere la intervención del usuario. Las entradas típicas necesarias son el número de pieza (P/N), el número de LOTE y los valores de las mediciones. El número de pieza y el número de LOTE se pueden introducir con un lector de código de barras o manualmente. Para realizar una entrada manual o si no se acepta la entrada del lector de códigos de barras, tocar **<edit>** en la barra de herramientas y utilice el campo de entrada.

Una vez finalizadas todas las acciones necesarias, se habilitará **<ok>** en la barra de herramientas. Para ir al siguiente paso, tocar **<ok>**. Para ir al paso anterior, tocar **<undo>**.



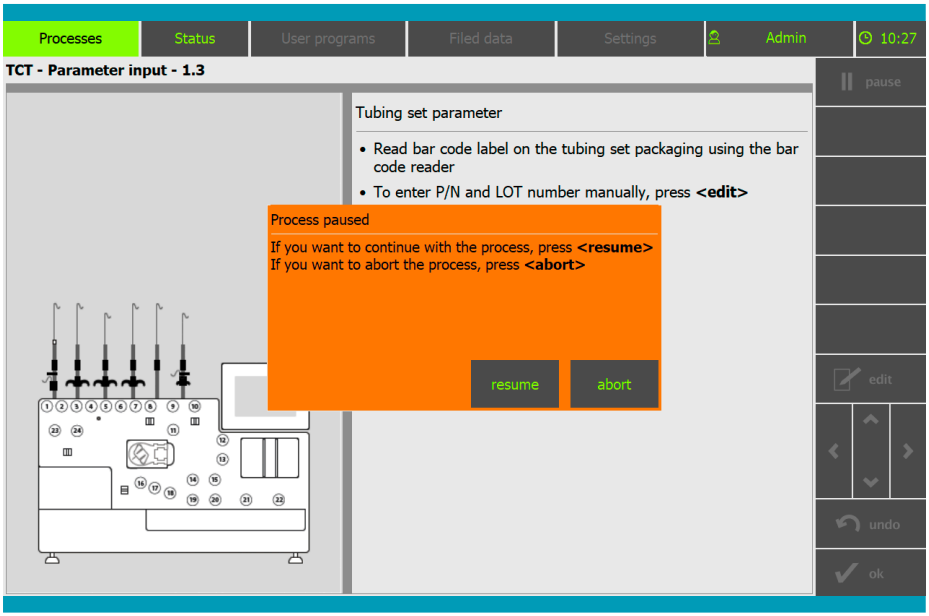
Pantalla 6.6: Ejemplo de paso en el proceso de aplicación TCT

6.8 Pausar un proceso de aplicación

Para pausar el proceso actual, tocar **<pause>** en la barra de herramientas. Aparecerá una ventana emergente (Pantalla 6.7). Para continuar un proceso en pausa, tocar **<resume>**. Para finalizar el proceso, tocar **<abort>**.

IMPORTANTE

Un proceso cancelado no se podrá reanudar.



Pantalla 6.7: Proceso pausado

6.9 Estado del instrumento y del proceso de aplicación

Para comprobar el estado operativo del proceso en curso, tocar <Status> en la barra de menús. El área de contenidos mostrará los elementos siguientes:

- Parámetros relacionados con el proceso: una lista de todos los parámetros relevantes del proceso (ver la Figura 6.1, a la izquierda).
- Cuadro de información y progreso: información relacionada con el proceso (ver la Figura 6.1, arriba a la derecha):
  - Nombre del operario
  - Información sobre la muestra
  - Progreso del subproceso y tiempo restante
  - Progreso del proceso y tiempo restante hasta la siguiente interacción del usuario
- Resumen gráfico: proporciona información visual sobre el estado del subproceso en curso del instrumento. (ver la Figura 6.1, abajo a la derecha). Todas las actividades de los componentes del instrumento (p. ej., bomba peristáltica, válvulas de pinzamiento) se visualizan en naranja.

Nota: La información de estado solo está disponible durante la ejecución de una aplicación. Esta página aparecerá en blanco cuando no se esté ejecutando ninguna aplicación. Es posible que no se disponga de un resumen gráfico para las CAP.

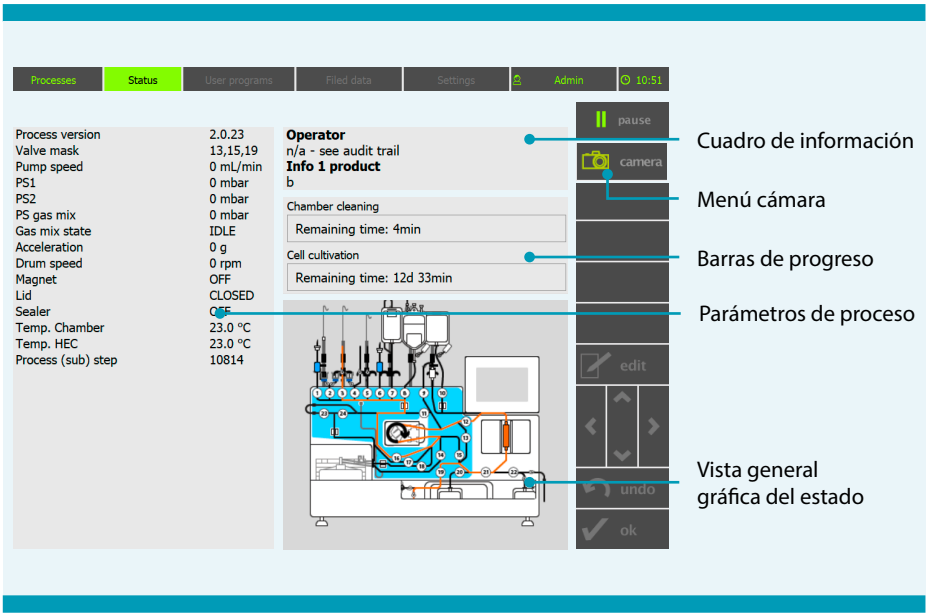


Figura 6.1: Resumen del estado del instrumento

6.10 Adquisición de imágenes

Con <camera> en la barra de herramientas se pueden seleccionar dos funcionalidades de cámara durante las aplicaciones seleccionadas (ver la Figura 6.1).

- Imagen de la cámara de detección de capas: esta imagen se puede utilizar para medir los volúmenes de las fracciones de centrifugación. Solo estará disponible en aplicaciones seleccionadas y únicamente para aplicaciones seleccionadas y durante el primer ajuste de volumen tras la carga de la muestra. (ver la Figura 6.2).
- Imagen del microscopio: esta imagen se puede utilizar para supervisar visualmente el cultivo celular. Solo está disponible durante los procedimientos de cultivo celular (ver la Figura 6.3).

El proceso de aplicación capturará y guardará automáticamente la imagen en el protocolo. Para ver imágenes, tocar <camera> en la barra de herramientas cuando esté seleccionado el menú <Status>. (ver la Figura 6.1). En función del paso del proceso de aplicación, el área de contenidos mostrará una imagen de la cámara de detección de capas o una imagen del microscopio.

Nota: La disponibilidad de <camera> en la barra de herramientas está controlada por el proceso de aplicación. Las imágenes se grabarán automáticamente durante una aplicación.

6.10.1 Cámara de detección de capas

El software detecta automáticamente las distintas capas. En la Figura 6.2 , las barras rojas y naranjas marcan la posición de las capas dentro de la imagen. Un diagrama debajo de la imagen muestra los valores registrados para los volúmenes de las fracciones de centrifugación. Las curvas se muestran en rojo y naranja de acuerdo con las barras dentro de la imagen (ver la Figura 6.2).



Figura 6.2: Resumen del estado del instrumento

Están disponibles las siguientes funciones:

- Grabación de imágenes: tocar <snap> en la barra de herramientas. Tras una breve fase de registro (aprox. 15 segundos), la imagen mostrada será reemplazada por una imagen recién registrada.
- Archivado de imágenes: tocar <save> en la barra de herramientas. La imagen registrada se integrará en el protocolo del propio proceso.
- Salir del menú de la cámara: tocar <ok> en la barra de herramientas.

Nota: La disponibilidad de los botones anteriores se controla por el proceso de aplicación.

6.10.2 Camera del microscopio

El menú de la cámara muestra la última imagen guardada de la cámara del microscopio integrado (ver la Figura 6.3).

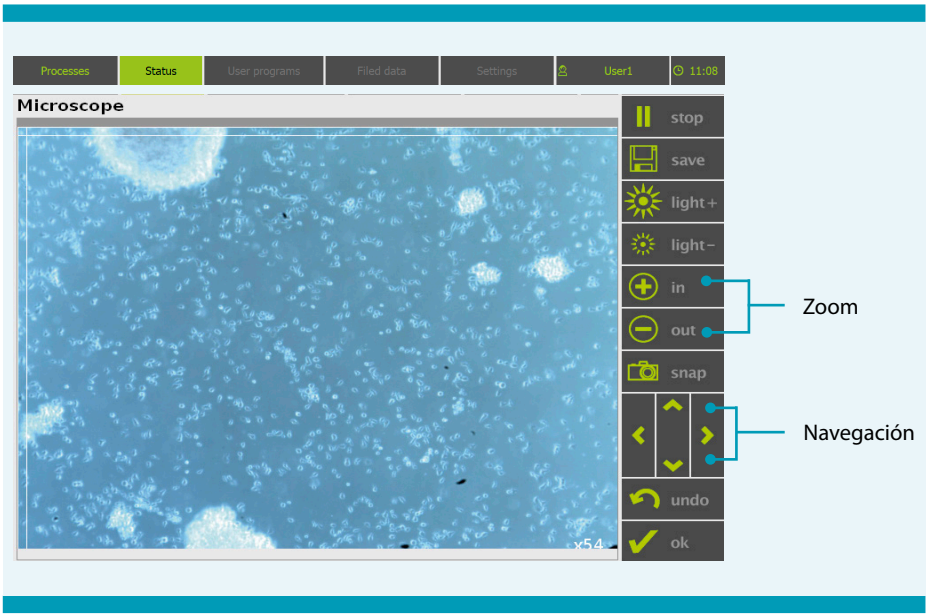


Figura 6.3: Pantalla del estado cuando la cámara microscopio está activa

Están disponibles las siguientes funciones:

- Ampliar imagen: Al tocar la imagen del microscopio, se ampliará el doble. El punto de tocar se convertirá en el nuevo centro de la imagen. La ampliación de las imágenes es de hasta 400 aumentos.
- Navegación dentro de una imagen: Al tocar un botón de navegación, se desplazará la imagen medio fotograma en la dirección seleccionada. Las barras de la imagen muestran la posición absoluta de la sección dentro de la imagen entera para facilitar la navegación. Tocar **<undo>** varias veces para deshacer los últimos diez pasos de navegación por separado.
- Grabación de imágenes: tocar **<snap>** en la barra de herramientas. Tras una breve fase de registro (aprox. 15 segundos), la imagen mostrada será reemplazada por una imagen recién registrada.
- Archivado de imágenes: tocar **<save>** en la barra de herramientas. La imagen registrada se integrará en el protocolo del propio proceso.
- Salir del menú de la cámara: tocar **<ok>** en la barra de herramientas.

Nota: La disponibilidad de los botones anteriores se controla por el proceso de aplicación.

7

Acceso a los datos

7.1 Recuperación de registros de aplicaciones

7.1.1 Visualización y exportación de archivos de registro a USB

El menú **<Filed data>** (Archivos) muestra el archivo de registro generado a partir de los procesos, las herramientas y los ajustes de la aplicación. En el área de contenidos, la lista de archivos muestra la hora, el nombre, el tipo, la duración y el estado de la ejecución del proceso (Pantalla 7.1).

Nota: El menú **<Filed data>** no está disponible durante la ejecución de un proceso. El botón correspondiente estará inactivo.

Visualización de archivos de registro

Para ver el contenido del archivo PDF del protocolo de proceso y del archivo PDF del anexo del protocolo, seleccionar el registro de destino y tocar **<ok>**.
(ver la Pantalla 7.1). El contenido del archivo seleccionado se mostrará en el área de contenidos (ver la Pantalla 7.2). Para volver a la lista de archivos, tocar **<ok>**.



Pantalla 7.1: Ejemplo de una lista de archivos



Pantalla 7.2: Ejemplo de un protocolo de proceso (aplicación TCT)

Exportación a una memoria USB flash

1. Insertar una memoria USB flash.
2. Abrir el archivo de registro de destino y tocar **<save>** en la barra de herramientas.

IMPORTANTE

- Asegurarse de que el nombre de la memoria USB flash no sea «netext», ya que este término está reservado para el software.
- Para hacer una copia de seguridad de todos los datos de proceso, se puede utilizar la herramienta Backup Filed Data (Copia de seguridad de los archivos), ver la sección 8.2.2 ´Backup Filed Data (Copia de seguridad de los archivos)´.
- La memoria USB flash debe presentar el formato FAT32 y no debe estar protegida por contraseña.

7.1.2 Recuperación por medio de FTP

FTP es un protocolo de red que permite la transferencia de datos entre el CliniMACS Prodigy (denominado servidor FTP) y el ordenador del usuario final (denominado cliente FTP) a través de conexiones IP (Internet Protocol, protocolo de Internet). Se puede acceder a todos los archivos de registro generados a partir de la ejecución de la aplicación.

Para acceder a los datos a través de FTP se requiere una configuración. A fin de configurar el instrumento para la conexión FTP, seguir las instrucciones de la sección 9.4.1 ´Configuración del instrumento´. Tras la configuración, el usuario puede conectarse al instrumento con cualquier cliente FTP disponible (p. ej., FileZilla) para descargar protocolos y archivos de registro; la Figura 7.1 muestra un ejemplo de parámetros de conexión. Para conectarse al instrumento, introducir los datos siguientes:

- La dirección IP del instrumento. Figura en **<Settings>** ▸ **<Tools>** ▸ **<Info>** ▸ **<Network information>**.
- El puerto: use el puerto predeterminado 21.
- Para el nombre de usuario y la contraseña se admiten dos opciones de inicio de sesión:
    - Opción de inicio de sesión 1: una cuenta registrada en el sistema de administración de usuarios (consultar el capítulo 10 ´Administración de usuarios´). En este caso, utilice la cuenta de usuario y la contraseña. El establecimiento y la finalización de la conexión se grabarán en el audit trail.

- Opción de inicio de sesión 2: un nombre de usuario y una contraseña locales guardados en FTP/File Share Settings (Ajustes de FTP/intercambio de archivos). La información de inicio de sesión figura en **<Settings>** ▸ **<Network Settings>** FTP/FS. En este caso, el establecimiento y la finalización de la conexión no se grabarán en el audit trail.

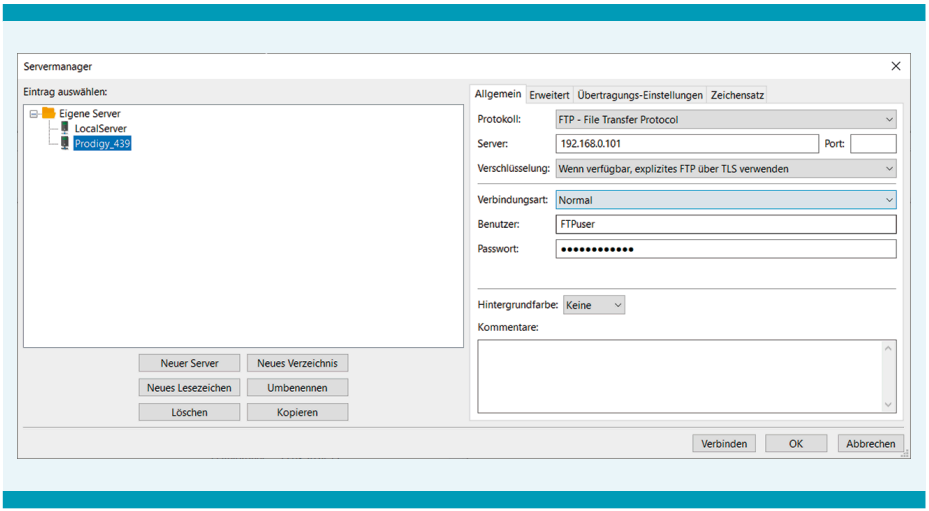


Figura 7.1: Ejemplos de parámetros de conexión

IMPORTANTE

- Si utiliza la opción de inicio de sesión 1, asegurarse de que la función «File management user» esté asignada a esta cuenta. Consultar la forma de asignar la función a la cuenta en el capítulo 10 «Administración de usuarios».
- El software no es compatible con FTP seguro (sFTP). Se recomienda utilizar el instrumento en una red segregada si se accede a los archivos a través de FTP.

Nota: Un usuario individual solo podrá establecer una única conexión a la vez, ya que el servidor del instrumento no permite conexiones múltiples. Si se utiliza un software cliente que utiliza conexiones simultáneas (p. ej., FileZilla), cambie los ajustes del cliente para permitir una sola sesión. De lo contrario, los contenidos solo se podrán examinar, pero no descargar.

7.1.3 Recuperar archivos a través de compartir archivos (File sharing)

Los archivos de registro generados durante la ejecución de la aplicación se pueden recuperar a través de una carpeta de red compartida. Una vez finalizada la ejecución de la aplicación, todos los archivos generados se colocarán automáticamente en una subcarpeta creada para cada instrumento dentro de la carpeta compartida.

Figura 7.2 muestra la estructura de archivos de la carpeta compartida. Para habilitar el intercambio de archivos es necesario configurarlo. Para configurar el intercambio de archivos, seguir las instrucciones en la sección 9.3 ´Conexión a una unidad de red´.

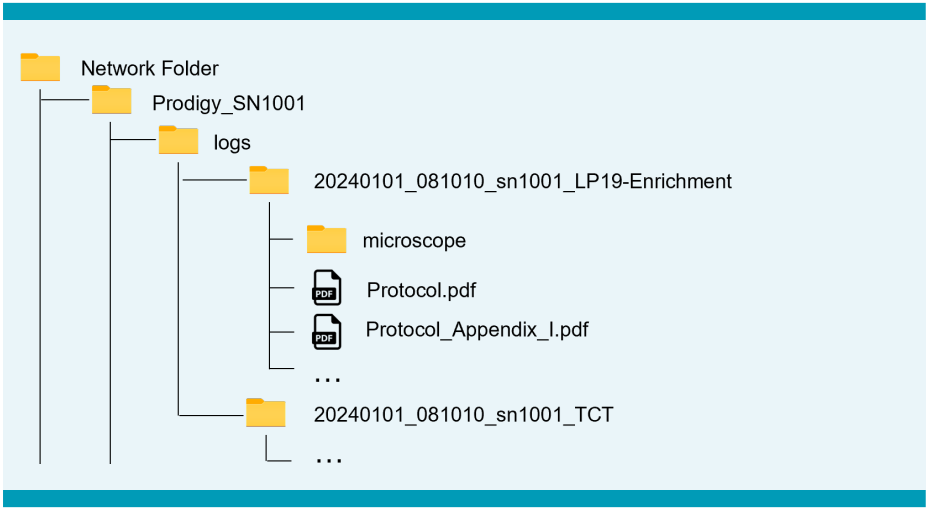


Figura 7.2: Estructura de los archivos compartidos

IMPORTANTE

Los archivos de registro guardados en el instrumento están protegidos mediante control de acceso para garantizar que solo tenga acceso personal autorizado. Una vez se transfieran estos archivos a una unidad de red, será responsabilidad del usuario aplicar las medidas de control de acceso adecuadas.

7.2 Recuperación del audit trail

El sistema de audit trail registra todas las interacciones de los usuarios con el software. Cada interacción del usuario da lugar a una audit trail que incluye el usuario ejecutor, el cronofechador y la descripción de la interacción. El audit trail se puede exportar en formato .pdf y .csv. Tabla 7.1 muestra el formato del audit trail.

IMPORTANTE

El cronofechador del audit trail es siempre la hora UTC.

Time (Hora)	Categoría	tipo	Usuario	Descripción
21-Jul-2020 10:33:44	Interacción del usuario	Cierre ventana emergente	AccountID	«Advertencia» de progreso pausado
..	..	..	..	..

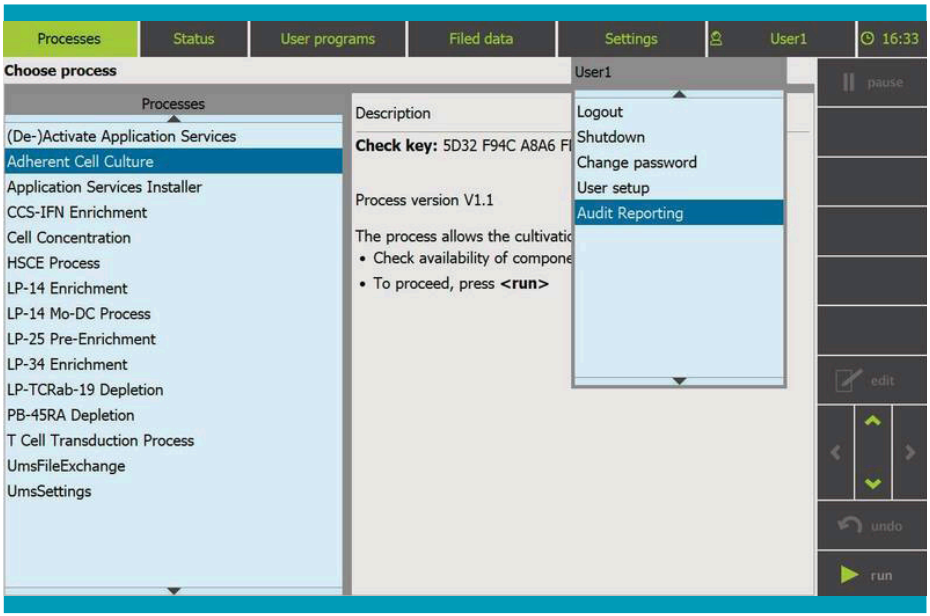
Tabla 7.1: Formato audit trail

Nota: Para acceder al sistema de audit trail se requiere la función «ATS User» o una función con derechos de «audit trail Management».

- La función «ATS User» dispone de acceso total, lo que permite ver, exportar y eliminar registros de audit trail.
- Se puede crear una nueva función para el acceso limitado a las funciones de audit trail. Consultar el capítulo 10 «Administración de usuarios» para más información sobre cómo configurar las funciones y los derechos.

7.2.1 Ver el audit trail

Para abrir el audit trail, ir a ▸ **<Audit Reporting>** (ver la Pantalla 7.3). El menú **<audit trail>** contiene una lista de todos los registros de audit trail disponibles en el instrumento (ver la Figura 7.3).



Pantalla 7.3: Registros de audit trail

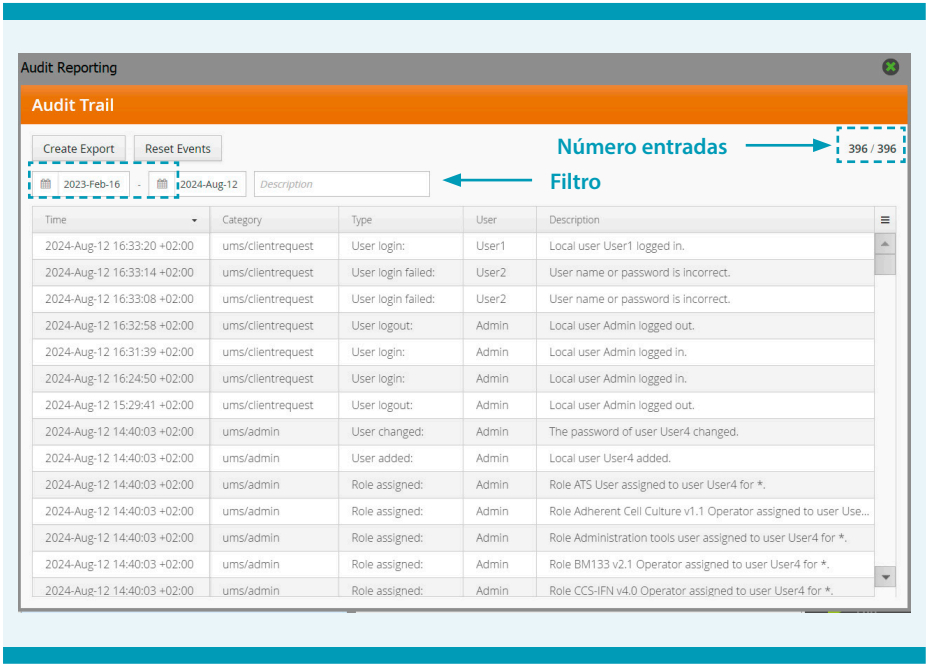
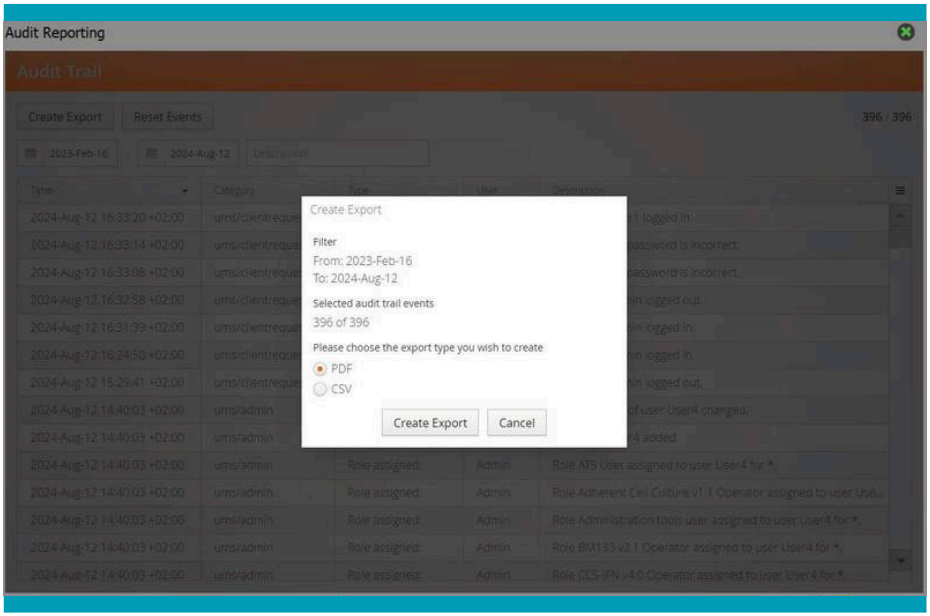


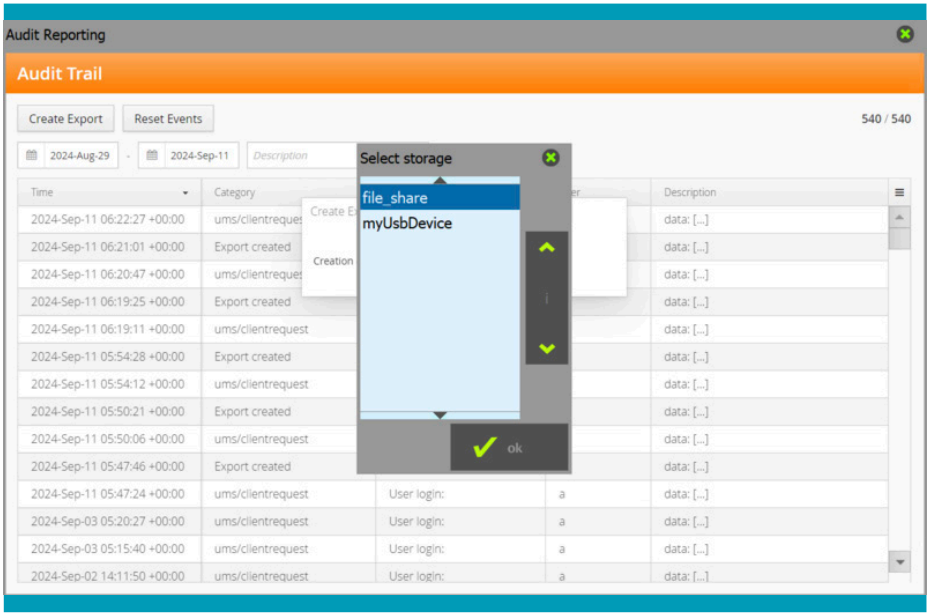
Figura 7.3: Menú audit trail

7.2.2 Exportar el audit trail

1. Introducir los criterios de filtrado en los campos de la Figura 7.3. Si no se introduce ningún criterio, se exportarán todos los registros.
2. Tocar **<Create Export>** situado encima de los criterios de filtrado. Aparecerá una ventana emergente (Pantalla 7.4).
3. Elegir el formato y tocar **<Create Export>** en la ventana emergente.
4. Si se detectan varios sitios de almacenamiento, p. ej., si está configurado el intercambio de archivos y se inserta una memoria USB flash, será necesario elegir el lugar de almacenamiento (Pantalla 7.5).



Pantalla 7.4: Creación de una exportación de audit trail



Pantalla 7.5: Selección del lugar de almacenamiento del audit trail

5. Esperar a que finalice el proceso y compruebe si el archivo se ha exportado.

7.2.3 Eliminación de un audit trail

1. Para eliminar todas las entradas de la pista de auditoría, tocar **<Reset Events>** (Restablecer eventos).

2. Confirmar con **<Continue Reset>**. Después del restablecimiento, se eliminan todos los registros. Se añade un nuevo registro para la acción de eliminación.

IMPORTANTE

No es posible eliminar entradas individuales. Los datos eliminados no se pueden restaurar. Asegúrarse de que solo los usuarios autorizados dispongan del derecho para eliminar el audit trail. Para configurar las funciones y los derechos, consultar el capítulo 10 «Administración de usuarios».

8

Herramientas y ajustes del usuario

8.1 Acceso a herramientas y ajustes de usuario

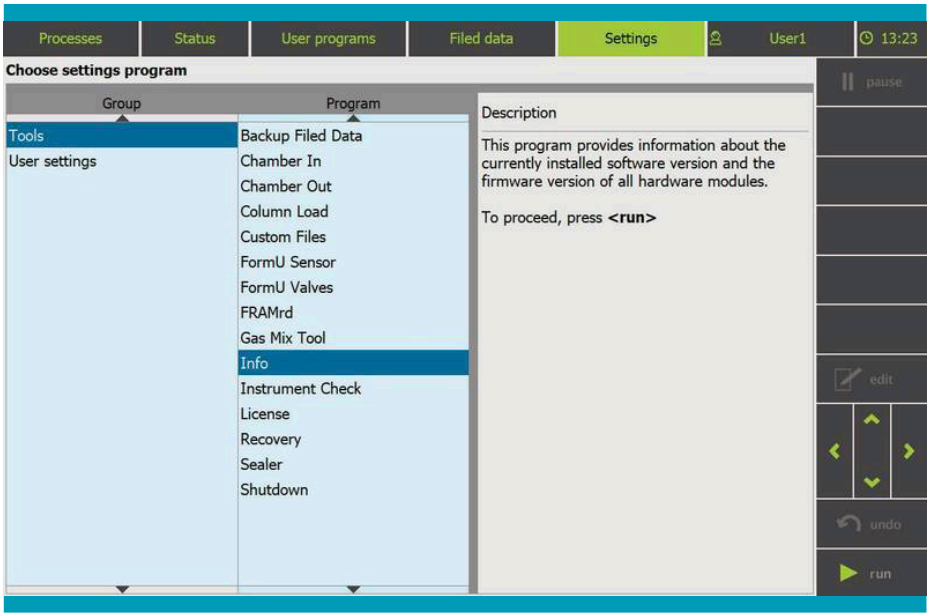
En el menú **<Settings>** figuran dos tipos de programas: herramientas y ajustes.

Nota: Las herramientas y los ajustes no están disponibles durante la ejecución de un proceso.

Para localizar y ejecutar una herramienta/un ajuste:

1. Seleccionar **<Tools>** o **<User settings>** de la lista de grupos, ver la Pantalla 8.1.
2. Tocar el programa deseado de la lista de programas. El programa seleccionado se resalta con fondo azul. En el campo de descripción encontrará información detallada sobre la herramienta/el ajuste seleccionados. Tocar ^ y v en la lista de procesos para desplazarse por más opciones. También puede utilizar los botones de navegación para localizar y seleccionar el programa.
3. Para iniciar el programa seleccionado, tocar **<run>** en la barra de herramientas.

En las siguientes secciones se presentarán las herramientas y los ajustes de usuario más utilizados.



Pantalla 8.1: Selección de una herramienta o de un ajuste

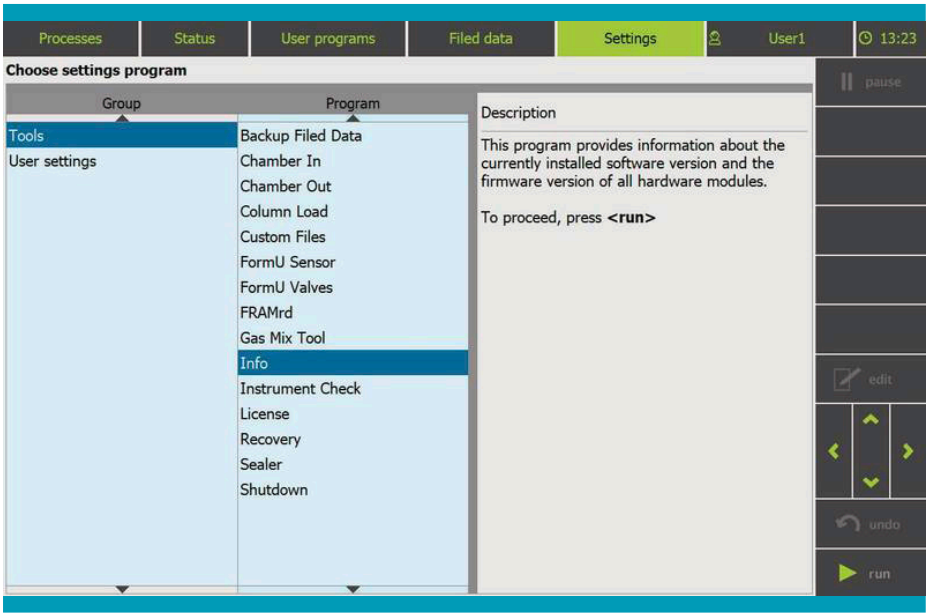
8.2 Tools (Herramientas)

Todas las herramientas figuran en <Settings> ▸ <Tools>.

8.2.1 Info tool (Información herramientas)

La información herramientas proporciona información detallada sobre el software y el hardware. La información importante incluye:

- Versión de software
- Número de compilación
- Versión del firmware
- Uso del espacio del disco duro, incluido el espacio restante, el espacio utilizado y el espacio total
- Dirección IP
- Dirección MAC
- Información completa sobre el tiempo de ejecución (incluidas todas las aplicaciones y herramientas), tiempo de inactividad (tiempo que el instrumento no estuvo ejecutando una aplicación)



Pantalla 8.2: Herramienta Info

8.2.2 Backup Filed Data (Copia de seguridad de los archivos)

La herramienta Backup Filed Data copia todos los datos del proceso a una ubicación de copia de seguridad o borra todos los datos del proceso.

IMPORTANTE

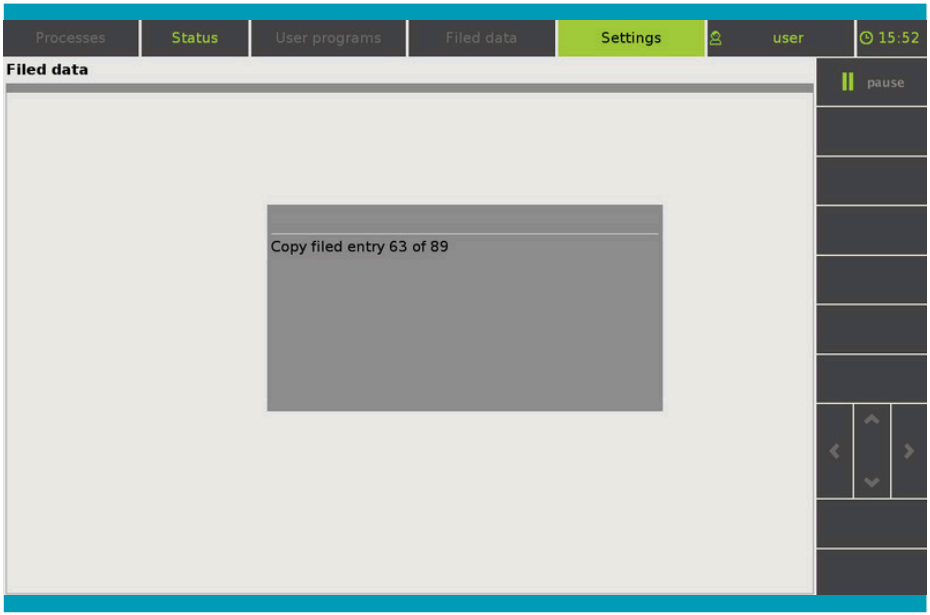
- Se recomienda realizar copias de seguridad de los datos del proceso con regularidad. De lo contrario, puede aparecer un mensaje indicando que no se debe iniciar el programa porque se ha alcanzado la capacidad máxima de almacenamiento de los datos archivados.
- Si utiliza una memoria USB flash para la copia de seguridad, la memoria USB flash debe presentar el formato FAT 32 y no debe estar protegida por contraseña.
- Si está configurado el uso compartido de archivos, los archivos también se pueden exportar a la carpeta de intercambio de archivos (ver la sección 9.3 ´Conexión a una unidad de red´).

Copia de datos

1. Insertar una memoria USB flash.
2. Ir a <Settings> ▸ <Tools> ▸ <Backup Filed Data>, y tocar <run>.
3. Seleccionar <Backup> en la ventana de instrucciones (ver la Pantalla 8.3). Se iniciará la copia (ver la Pantalla 8.4).

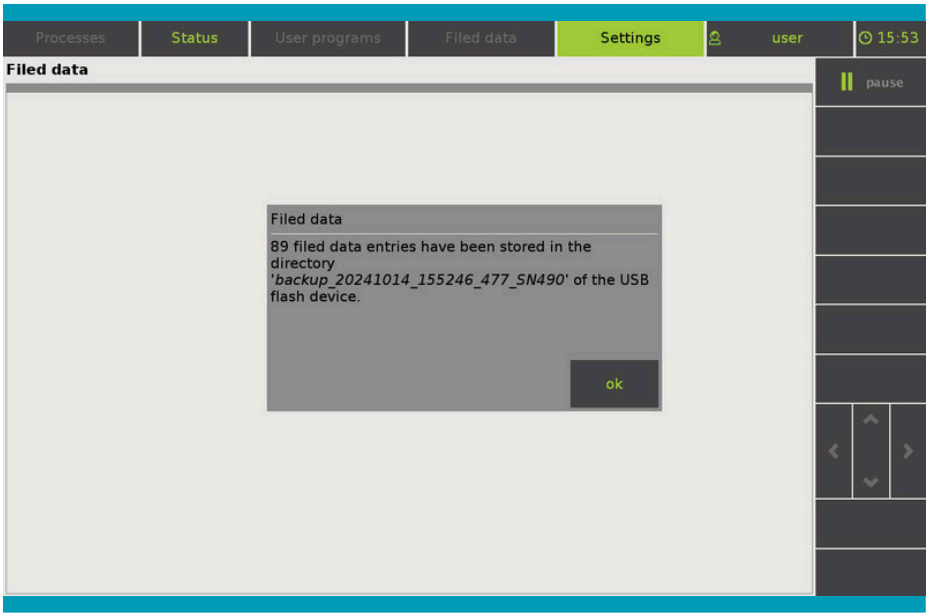


Pantalla 8.3: Selección de copia de seguridad



Pantalla 8.4: Proceso de copia de seguridad

4. Esperar a que finalice la copia y tocar <ok> en la ventana de instrucciones (ver la Pantalla 8.5).
5. Verificar que los archivos se hayan descargado completamente.



Pantalla 8.5: Copia de seguridad finalizada

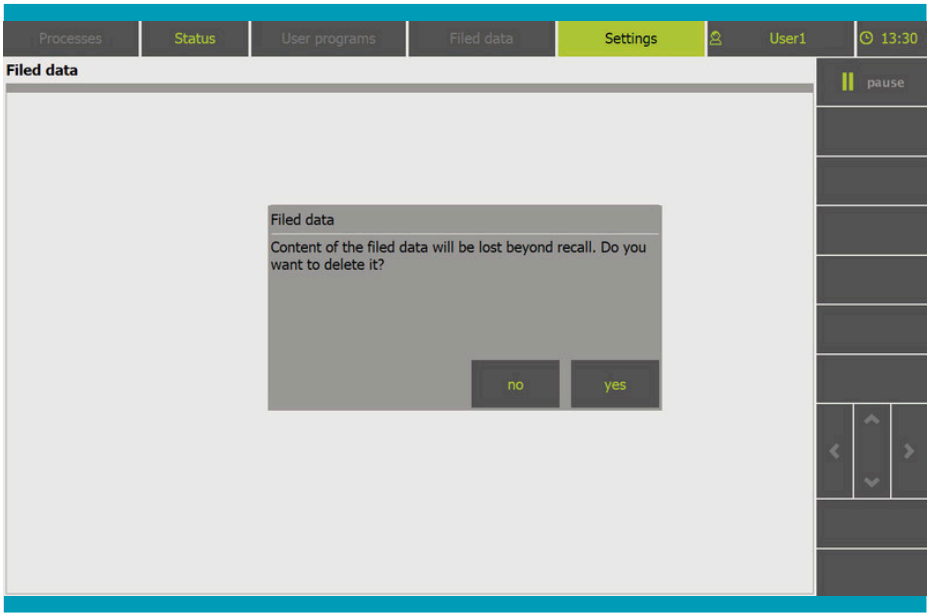
Eliminación de datos

1. Verificar que los archivos se hayan descargado completamente.
2. Ir a <Settings> ▸ <Tools> ▸ <Backup Filed Data>, y tocar <run>.
3. Tocar <Delete> (ver la Pantalla 8.6).



Pantalla 8.6: Selección de «Delete»

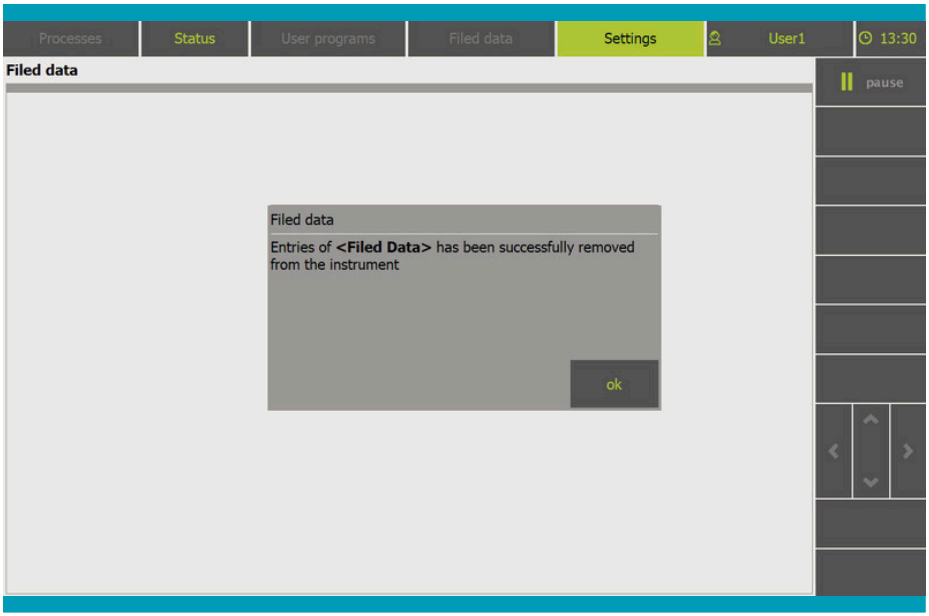
4. Para confirmar tocar <yes> (ver la Pantalla 8.7).



Pantalla 8.7: Confirmación de la eliminación de datos

5. Esperar a que finalice el proceso de eliminación y tocar <ok> en la ventana de instrucciones (ver la Pantalla 8.8).
6. Se eliminarán todos los registros de <Filed Data>. Se creará un registro para ejecutar la herramienta Backup Filed Data.

IMPORTANTE
Los datos eliminados no se pueden restaurar.



Pantalla 8.8: Eliminación finalizada

8.2.3 Chamber In (Introducir cámara)

Esta herramienta sirve para insertar la unidad CentriCult fuera de una aplicación en ejecución. El adaptador de bloqueo de la cámara se desplaza a la posición de inserción y desbloquea la tapa de la unidad CentriCult. Después de ejecutar esta herramienta, abra la unidad CentriCult manualmente.

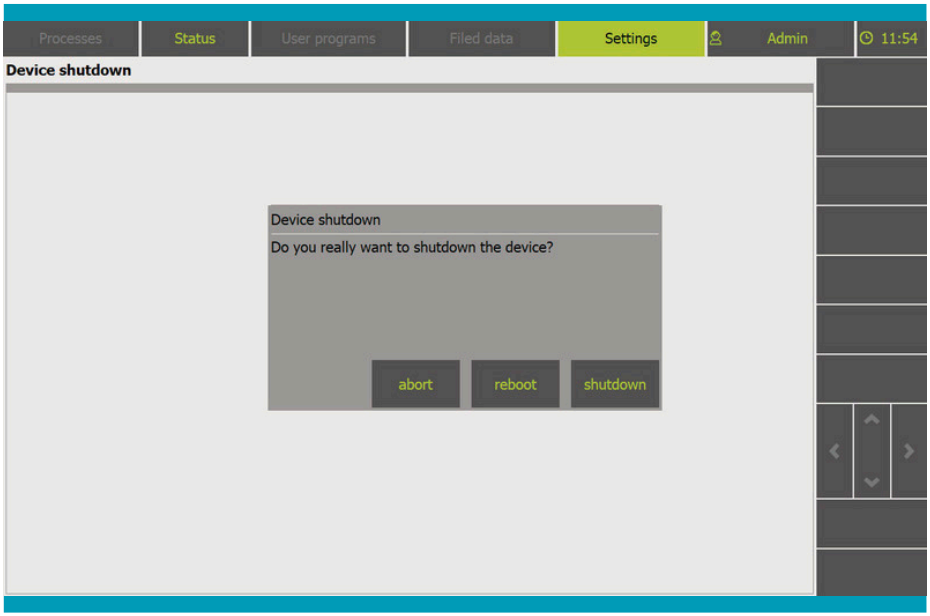
8.2.4 Chamber Out (Extraer cámara)

Esta herramienta sirve para sacar la unidad CentriCult fuera de una aplicación en ejecución. El adaptador de bloqueo de la cámara se desplaza a la posición de intercambio y desbloquea la tapa de la unidad CentriCult. Después de ejecutar esta herramienta, abra la unidad CentriCult manualmente.

8.2.5 Shutdown (Apagar)

Esta herramienta apagará o reiniciará el instrumento.

1. Tocar **<run>** en la barra de herramientas para ejecutar la función de apagado.
2. Seleccionar abort (cancelar), shutdown (apagar) o reboot (reiniciar) (ver la Pantalla 8.9).



Pantalla 8.9: Selección de shutdown (apagar) o reboot (reiniciar)

8.2.6 Recovery (Recuperación)

Este programa permite recuperar productos celulares en una bolsa determinada en caso de fallo del proceso. Esta herramienta solo es compatible con los siguientes sets de tubos CliniMACS Prodigy: TS 310, TS 500 y TS 510.

IMPORTANTE

Utilice esta herramienta únicamente siguiendo las instrucciones de Miltenyi Biotec Technical Support.

8.2.7 Herramienta Gas Mix (Mezcla de gases)

Este programa permite tomar muestras de gas con una bolsa de muestras de la unidad de mezcla de gases.

8.2.8 Herramienta Instrument Check (Chequeo del instrumento)

Esta herramienta realiza una comprobación semiautomatizada del instrumento con cierta interacción necesaria por parte del usuario.

8.2.9 Column Load (Carga columna)

En algunos casos específicos, el proceso permite el enriquecimiento de células CD34 positivas de productos de leucaféresis.

8.2.10 Custom Files (Archivos personalizados)

Este programa se utiliza para añadir CAPs al instrumento.

8.2.11 Sealer (Sellador)

Este programa permite encender y apagar el sellador.

8.3 User settings (Ajustes de usuario)

Los ajustes figuran en **<Settings>** ▸ **<User settings>**.

8.3.1 Set time (Ajustar hora)

Esta función permite ajustar la fecha y la hora en el instrumento.

Nota: La hora aquí ajustada se sobrescribirá automáticamente si está activada la sincronización horaria de la red. Para configurar la sincronización horaria de la red, ver la sección 9.6 ´Activación de la sincronización horaria de la red´.

8.3.2 Network settings (Ajustes de red)

Este ajuste contiene información necesaria para la integración en la red. Para una explicación detallada ir a las secciones siguientes:

- 9.1 para la integración en la red
- 9.2 para la conexión LDAP
- 9.3 para compartir archivos
- 9.4 para la transferencia de archivos por FTP
- 9.6 para la sincronización horaria de la red

Para configurar la notificación por correo electrónico, ver la sección 9.5 ´Conexión a un servidor de correo electrónico´

8.3.3 Custom settings (Ajustes personalizados)

Los ajustes personalizados son ajustes generales para el instrumento, como el idioma, el nombre de la empresa, el departamento, la calle, el código postal, la ciudad, el nombre del instrumento, la persona de contacto y la ubicación.

El ajuste de notificación por correo electrónico también se puede encontrar en Customer Settings, ver la sección 9.5 ´Conexión a un servidor de correo electrónico´.

8.3.4 Module Settings (Ajustes del módulo)

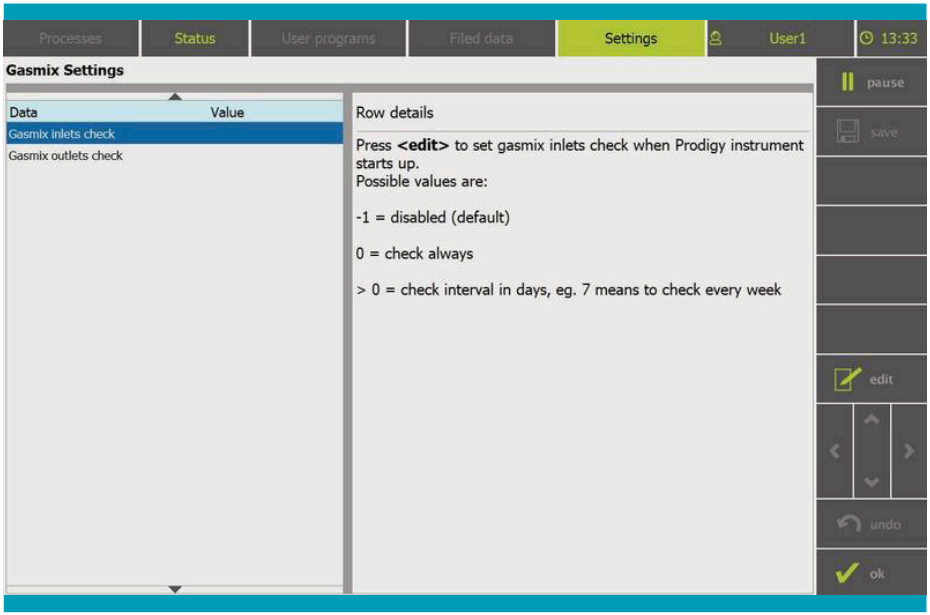
Los ajustes del módulo contienen configuraciones para pruebas de hardware e incluyen:

- Comprobación de las entradas de mezcla de gases
- Comprobación de las salidas de mezcla de gases
- Comprobación de rotación
- Recordatorio de Supplementary Bag

Para cada uno de esos componentes, se puede ajustar que las comprobaciones se realicen en intervalos temporales diferentes:

- Nunca (-1)
- Siempre (0)
- Periódicamente (introducir el número en días).

Para un ejemplo de la configuración de las entradas de mezcla de gases ver la Pantalla 8.10.



Pantalla 8.10: Comprobación de la entrada de mezcla de gases

8.3.5 Herramienta Settings exchange (Ajustes del intercambio)

La herramienta <Settings Exchange> permite copiar configuraciones en varios instrumentos. Estos ajustes incluyen:

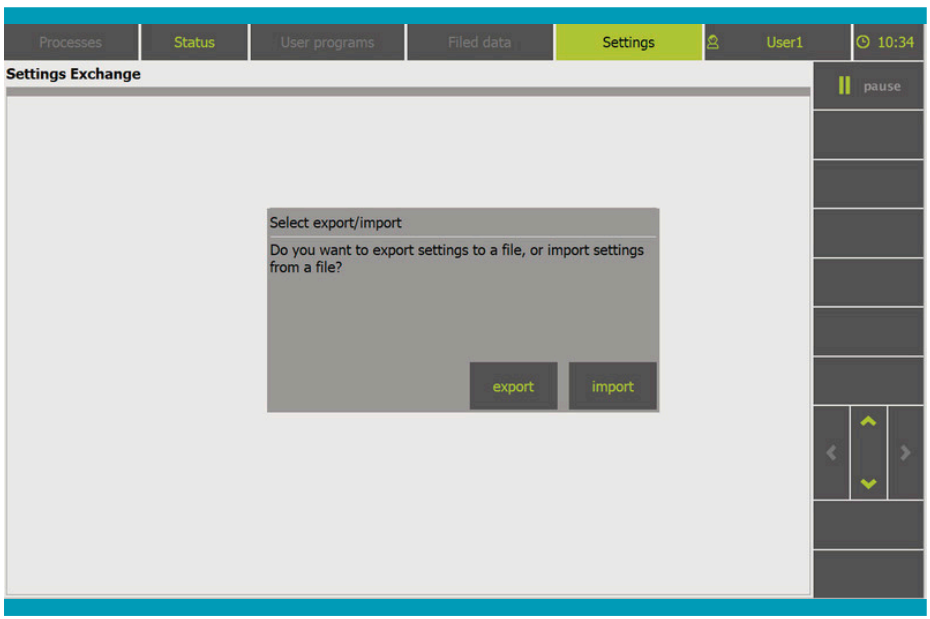
- Customer settings (Ajustes personalizados)
- Gasmix settings (Ajustes de mezcla de gases)
- Module settings (Ajustes del módulo)
- Network settings (Ajustes de red)

IMPORTANTE

- Si utiliza una memoria USB flash para la importación o exportación, la memoria USB flash debe presentar el formato FAT 32 y no debe estar protegida por contraseña.
- Si está configurado el uso compartido de archivos, los archivos también se pueden exportar a la carpeta de intercambio de archivos (ver la sección 9.3 ´Conexión a una unidad de red´).

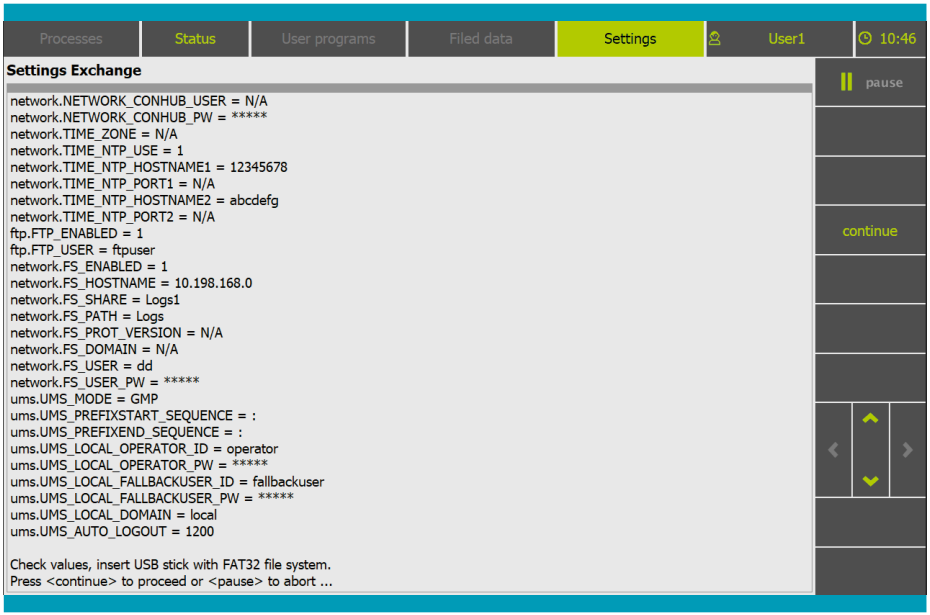
Ajustes para la exportación a una memoria USB flash

1. Insertar una memoria USB flash.
2. Ir a <Settings> ▸ <User settings> ▸ <Setting Exchange> y tocar <run>.
3. Tocar <export> en la ventana de instrucciones (ver la Pantalla 8.11).



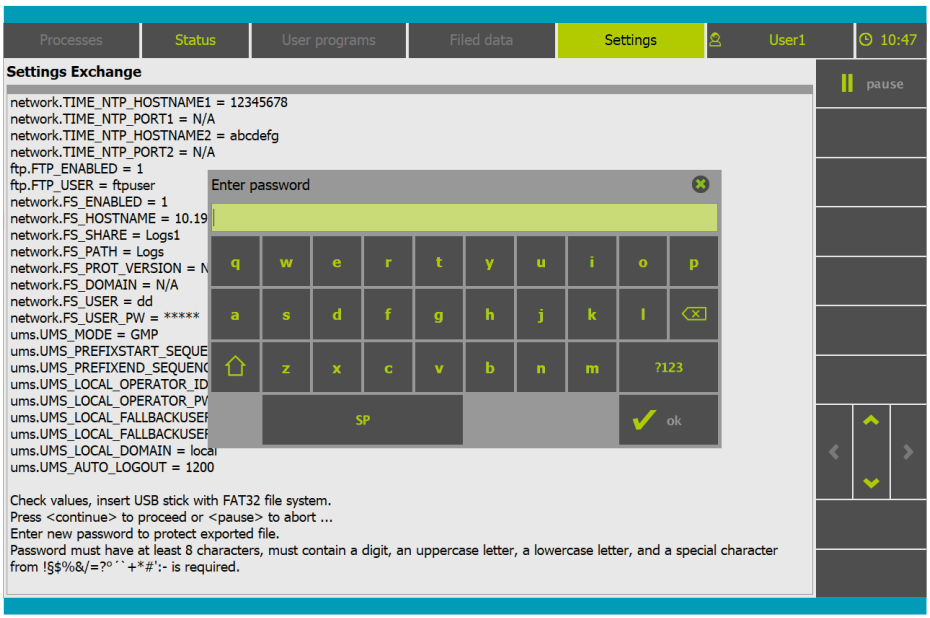
Pantalla 8.11: Selección de «export»

4. Compruebe los valores en pantalla. Tocar <continue> en la barra de herramientas.



Pantalla 8.12: Comprobación de los valores de ajuste

5. Introducir la contraseña de inicio de sesión.



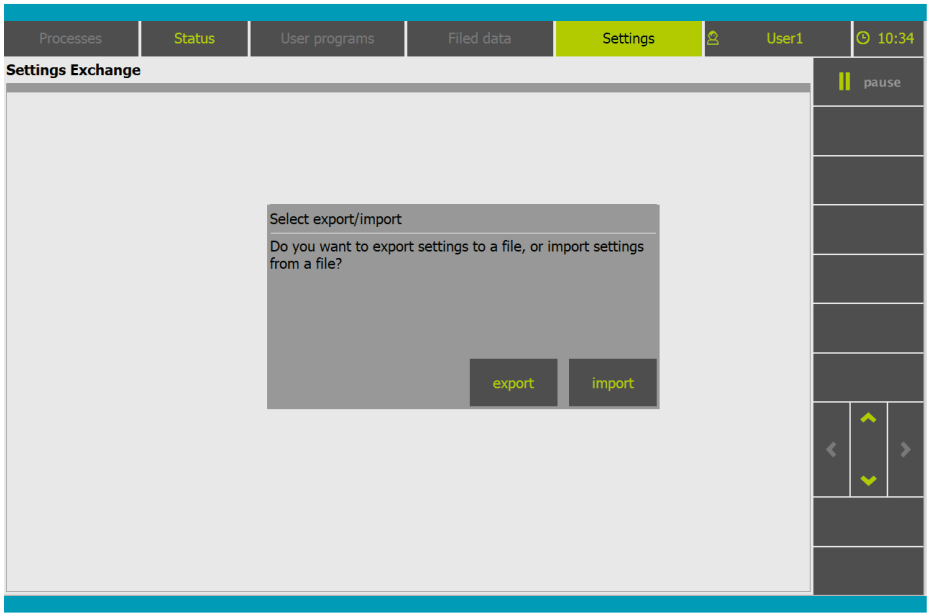
Pantalla 8.13: Introducción de la contraseña

Importar ajustes de la memoria USB flash

1. Insertar una memoria USB flash que contenga el archivo con los ajustes de usuario deseados.

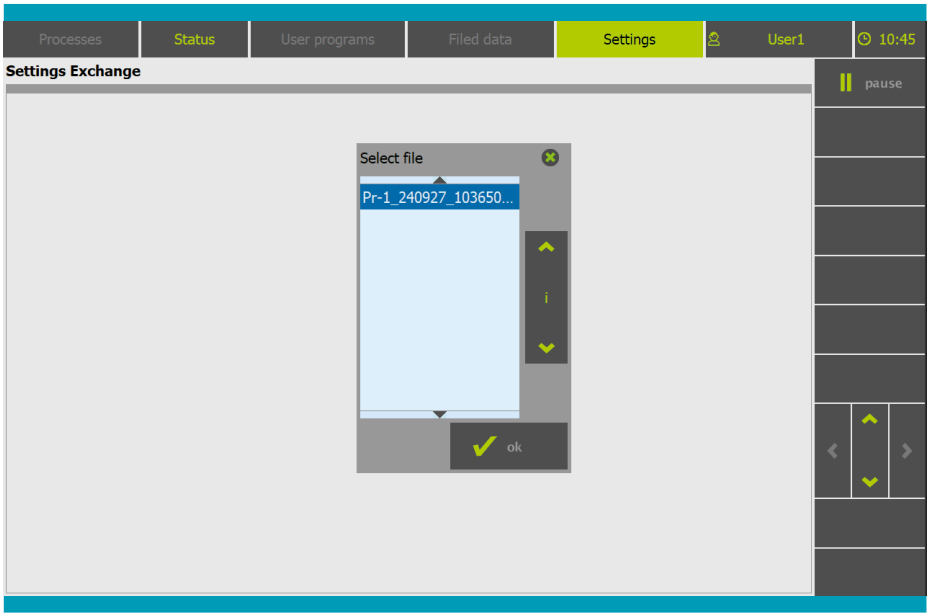
   Nota: La memoria USB flash debe presentar el formato FAT 32 y no debe estar protegida por contraseña.

2. Ir a <Settings> ▸ <User settings> ▸ <Setting Exchange> y tocar <run>.
3. Seleccionar <Import> en la ventana de instrucciones (ver la Pantalla 8.14).



Pantalla 8.14: Selección de «import»

4. Seleccionar los archivos que desee importar y tocar <ok> (ver la Pantalla 8.15).



Pantalla 8.15: Selección del archivo a importar

5. Introducir la contraseña de inicio de sesión (ver la Pantalla 8.13).

8.3.6 SetVolume (Ajustar el volumen)

Este programa ajusta el volumen del altavoz del instrumento.

8.3.7 N_2 Settings (Ajustes N_2)

Este programa configura que dos de las tres conexiones de gas del instrumento se van a utilizar (N_2, CO_2, aire comprimido).

9

Integración en la red

El instrumento se puede conectar a la red local mediante un adaptador USB-Ethernet. Para utilizar las siguientes funciones, se requiere una integración de red adecuada:

- Administración de usuarios centralizada (LDAP)
- Transferencia de archivos por FTP
- Intercambio automático de archivos
- Notificación por correo electrónico
- Sincronización horaria de la red

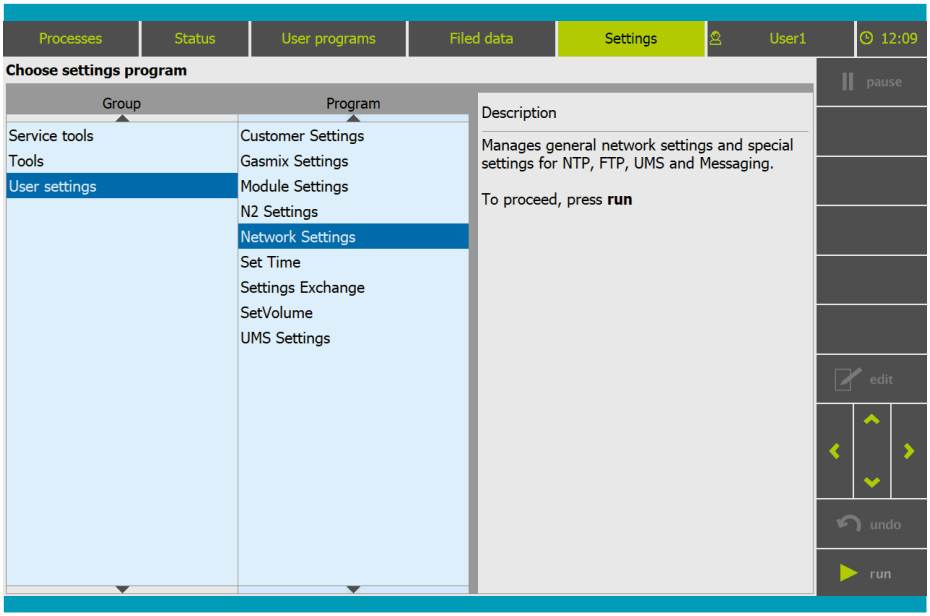
Para utilizar las funciones mencionadas, conectar primero el instrumento a la red local, ver la sección 9.1 ´Conexión a una red local´y seguir las instrucciones de las funciones específicas.

IMPORTANTE

- Solo los usuarios del UMS con la función de administrador «Administration tools user» o los usuarios con derechos de «Network Setting» tendrán acceso a este ajuste. Para configurar los derechos y las funciones, consultar el capítulo 10 «Administración de usuarios».
- En la pantalla puede aparecer el botón **<Connectivity Hub>**, pero actualmente está desactivado y permanecerá así hasta que se admita esta función.
- El usuario debe asegurarse de que la configuración del cortafuegos permita el intercambio de datos entre el instrumento y el servidor/cliente deseado. El cliente es responsable de la configuración de los parámetros del cortafuegos.
- Determinados cambios de los ajustes requieren reiniciar el instrumento para aplicarlos.

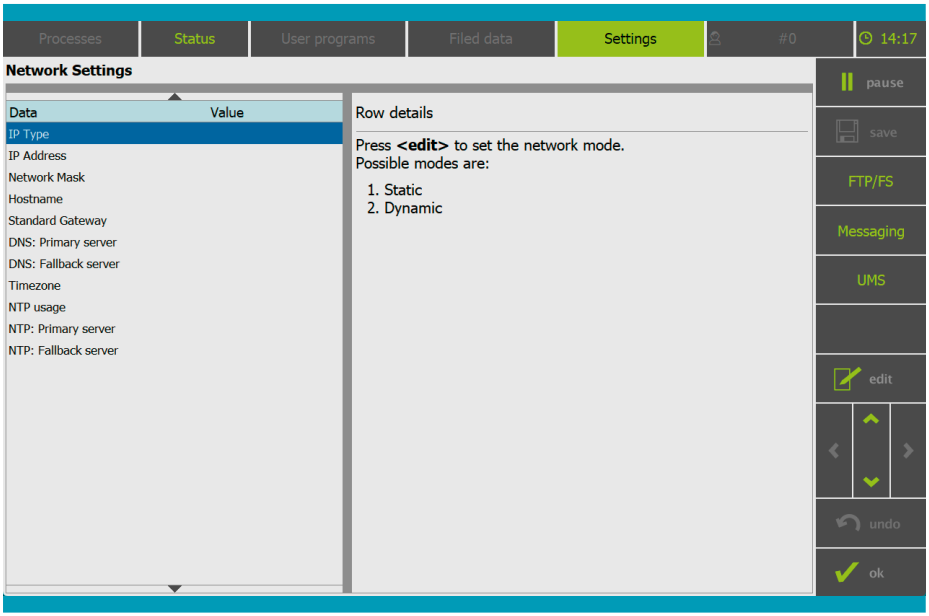
9.1 Conexión a una red local

1. Conectar el instrumento a la red local mediante un adaptador USB-Ethernet.
2. Para introducir los ajustes de red, ir a <Settings> ▸ <User settings> ▸ <Network Settings> y tocar <run> (ver la Pantalla 9.1). Se mostrarán los ajustes de red (Pantalla 9.2).



Pantalla 9.1: Selección de los ajustes de red

3. Para elegir entre una dirección IP estática y una dirección IP dinámica, seleccionar <IP Type> en la lista y tocar <edit> en la barra de herramientas e introducir el valor deseado en el campo de entrada.



Pantalla 9.2: Ajustes de red

Para direcciones IP estáticas, seguir estos pasos:

1. Seleccionar <IP Address> en la lista, tocar <edit> en la barra de herramientas e introducir la dirección IP en el campo de entrada.
2. Seleccionar <Network Mask> en la lista, tocar <edit> e introducir la máscara de red en el campo de entrada.
3. Para introducir el nombre del instrumento, seleccionar <Hostname> y tocar <edit>.
4. Para introducir la dirección IP de la puerta de enlace, seleccionar <Standard Gateway> y tocar <edit>.
5. Opcional: Para elegir la zona horaria, seleccionar <Timezone> y tocar <edit>. La zona horaria predeterminada del instrumento es Tiempo Universal Coordinado (UTC, por sus siglas en inglés).
6. Verificar que el instrumento esté conectado a la red local.

Para direcciones IP dinámicas, siga estos pasos:

1. Para introducir el nombre del instrumento, seleccionar <Hostname> y tocar <edit>.
2. El servidor dinámico se debe configurar. Introducir una dirección IP para el servidor principal (primary) y el servidor secundario (fallback).
3. Opcional: Para elegir la zona horaria, seleccionar <Timezone> y tocar <edit>.

La zona horaria predeterminada del instrumento es Tiempo Universal Coordinado (UTC, por sus siglas en inglés)

4. Verificar que el instrumento esté conectado a la red local.

IMPORTANTE

Si los puertos de red de su organización están protegidos por filtros de direcciones MAC, póngase en contacto con su proveedor local de servicios informáticos para configurarlos correctamente.

9.2 Conexión a un servidor LDAP

Para configurar la conexión con el servidor LDAP, ir a (menú de acceso rápido) y seleccionar <User Management>. En el menú <User Management>, seleccionar <Configuration> ▸ <LDAP Configuration>. Para configurar LDAP, seguir estos pasos (ver la Figura 9.1).

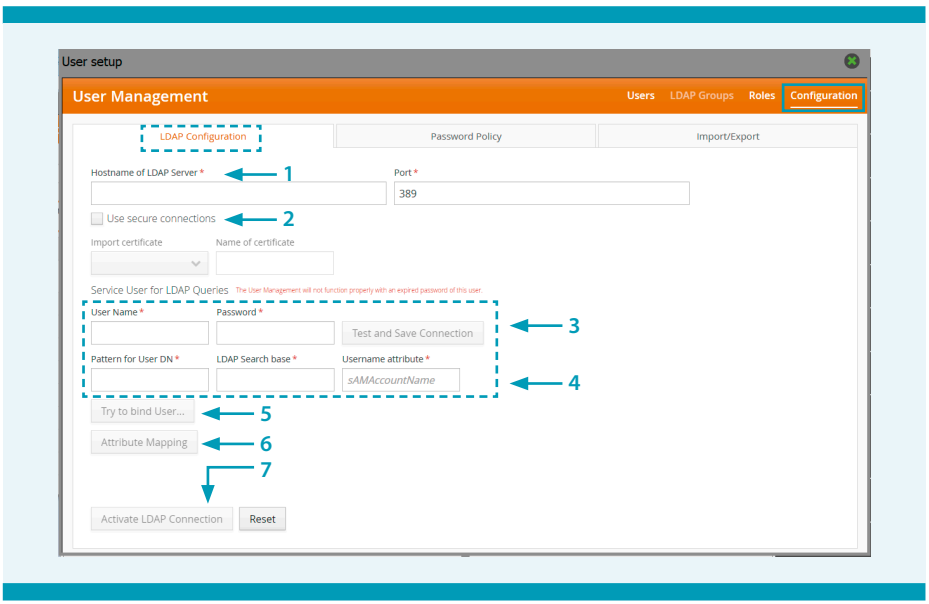


Figura 9.1: Menú «User Management» y pasos necesarios para configurar LDAP

1. Introducir el nombre de host/dirección IP del servidor LDAP.
2. Selección en caso necesario una conexión segura. Se ajustará automáticamente el puerto del valor predeterminado 389 al puerto 636 para una conexión LDAP segura. Para una conexión segura, seguir las instrucciones de la sección 10.4.2 ´Importar ajustes del UMS´ para importar el certificado en Prodigy Instrument y seleccionarlo en la lista desplegable <import certificate>.
3. Introducir el nombre de usuario y la contraseña de una cuenta LDAP válida. Se

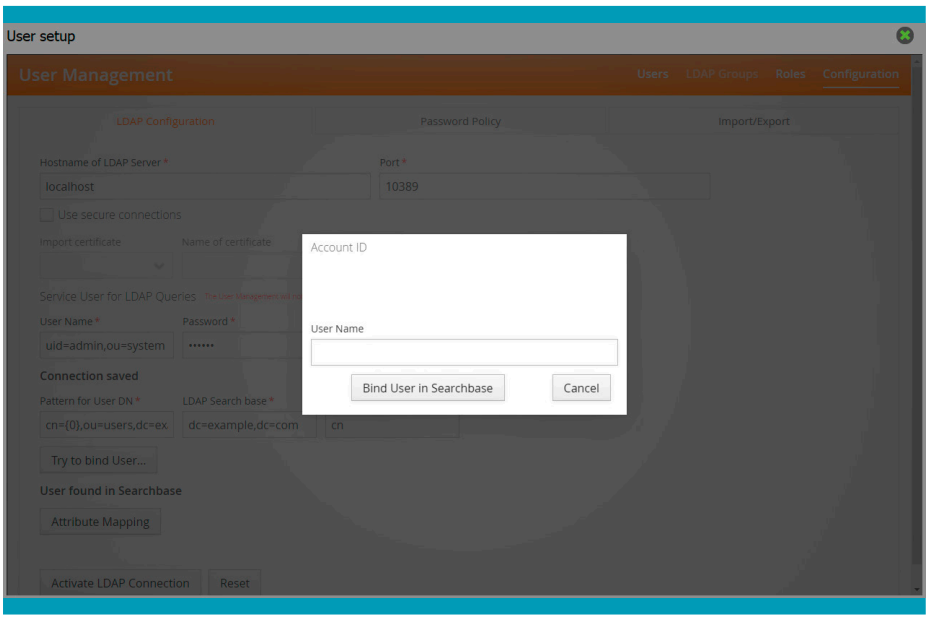
debe introducir la ruta LDAP completa del nombre de usuario. Tocar <Test and Save Connection>. Aparecerá una ventana emergente indicando que la conexión se ha establecido correctamente.

4. Introducir el patrón, la base de búsqueda y el atributo del nombre de usuario. El patrón para el nombre de dominio del usuario debe incluir la ruta completa. Estas entradas dependen de la estructura organizativa LDAP del usuario y del nombre de dominio. Para ver una breve explicación y ejemplos de valores típicos, pase el ratón sobre los cuadros de texto. Podría ser útil contar con una persona que tenga acceso a un programa de navegación LDAP para visualizar las unidades organizativas allí disponibles.

Los valores típicos son, por ejemplo:

- Patrón = <domain>/{0}, por ejemplo «nombre cliente_dev/{0}»
- Base de búsqueda = «OU=organización,DC=nombre cliente»
- Atributo del nombre de usuario = «sAMAccountName»

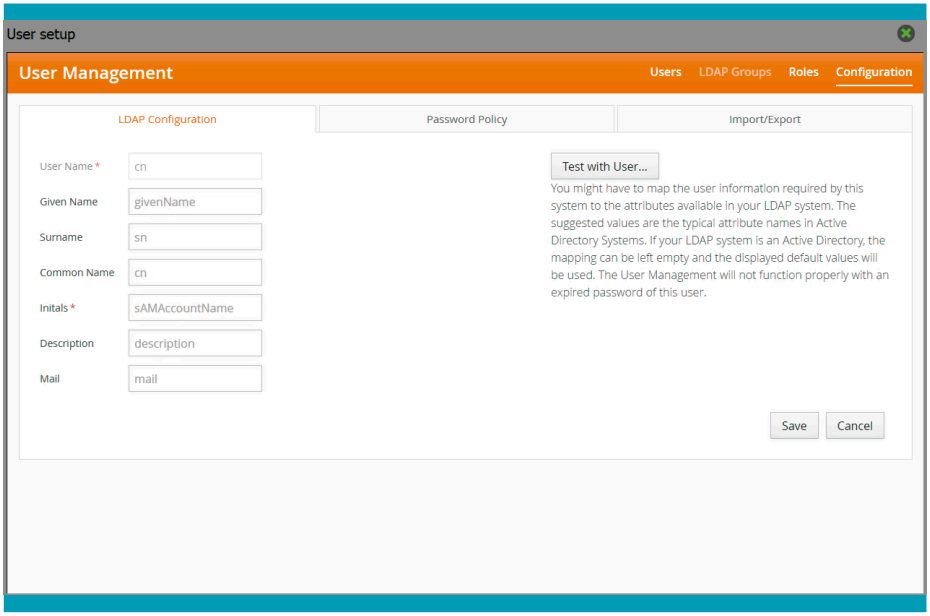
5. Tocar <Try to bind User..>. Aparecerá una ventana emergente (Pantalla 9.3). Introducir un nombre de usuario válido (el nombre de usuario puede ser el mismo utilizado para la prueba de inicio de sesión). Después, tocar <Bind User in Searchbase> para continuar. Si la introducción ha sido correcta, se cerrará la ventana emergente de ID de cuenta; de lo contrario, se mostrará un mensaje de error.



Pantalla 9.3: Ventana emergente para introducir un nombre de usuario válido

6. Tocar <Attribute Mapping>. Se mostrará la asignación de atributos (Pantalla 9.4). El atributo del nombre de usuario introducido en el paso 4 se asignará automáticamente al nombre de usuario. Introducir el mismo valor para «Initials» (Iniciales) que para «User Name» (Nombre usuario). La introducción de valores en este campo rellenará automáticamente parte de la información cuando se cree un usuario. Tocar <Save> para volver a la página de configuración de LDAP.

7. Tocar <Activate LDAP Connection>. Este botón estará activo si los pasos 3, 4 y 5 se han realizado correctamente.



Pantalla 9.4: Ejemplo de atributos prellenados

IMPORTANTE

Es necesario ajustar un valor para «Initials» (ver Pantalla 9.4), ya que este valor se considera información obligatoria para los usuarios del CliniMACS Prodigy. La falta de configuración o la configuración incorrecta del mapa de atributos puede provocar fallos en el inicio de sesión.

Estos siete pasos (ver la Figura 9.1) permiten configurar completamente la conexión LDAP que se podrá utilizar a continuación para crear grupos LDAP y usuarios LDAP en <User Management>. Encontrará más información sobre la administración de cuentas y funciones en el capítulo 10 ´Administración de usuarios´.

9.3 Conexión a una unidad de red

El intercambio de archivos automático enviará todos los archivos de registro a la unidad de red tras la ejecución del proceso, inmediatamente después de que finalice la aplicación. Los registros de audit trail también se pueden exportar a la unidad de red manualmente por medio de la intervención del usuario (ver la sección 7.2.2 ´Exportar el audit trail´). La transferencia automática de archivos está implementada en base al protocolo SMB (Server Message Block). Las versiones admitidas del protocolo SMB incluyen SMB 1.0, SMB 2.1 y SMB 3.0 (por defecto).

Nota: Se recomienda SMB 2.0 y SMB 3.0. SMB 1.0 solo se admite por razones de herencia y solo se deberá utilizar para interactuar con equipos heredados.

Prerrequisitos

- Servidor SMB: asegurarse de que este servidor SMB sea accesible. Compruebe la versión del protocolo SMB de este servidor antes de comenzar.
- Crear una carpeta previamente en el servidor SMB para el almacenamiento de datos. Anote el nombre del recurso compartido. Puede ser un recurso compartido anónimo (accesible para una cuenta de invitado) o un recurso compartido autenticado (accesible solo para una cuenta especificada).

Nota: Se recomienda el uso de un recurso compartido autenticado para la seguridad de los datos.

- Si se utiliza un recurso compartido autenticado, se requerirá una cuenta protegida por contraseña. Esta cuenta deberá tener acceso de lectura y escritura a la carpeta compartida en el servidor SMB.
- El instrumento está conectado a Ethernet y la red está habilitada.

Configuración del instrumento

Nota: Es importante introducir todos los parámetros de intercambio de archivos antes de activar la opción de uso compartido de archivos, ya que cualquier cambio posterior desactivará el intercambio de archivos. Después de configurar los ajustes, el instrumento se deberá reiniciar para finalizar la configuración. Los cambios realizados en la configuración de transferencia de archivos se aplicarán durante el reinicio.

1. Para abrir FTP/File Share Settings (Ajustes de FTP/intercambio de archivos), tocar **<FTP/FS>** en la barra de herramientas (Pantalla 9.2).
2. En **<FTP/File Share Settings>** solo son relevantes para el intercambio de archivos los parámetros del cuadro azul (ver la Figura 9.2).

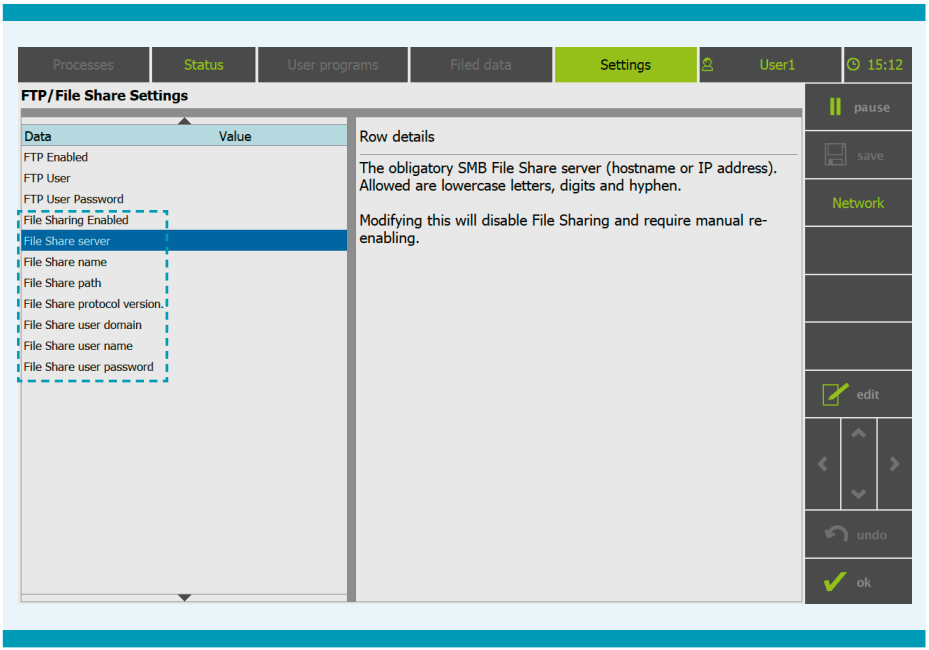


Figura 9.2: Parámetros de intercambio de archivos

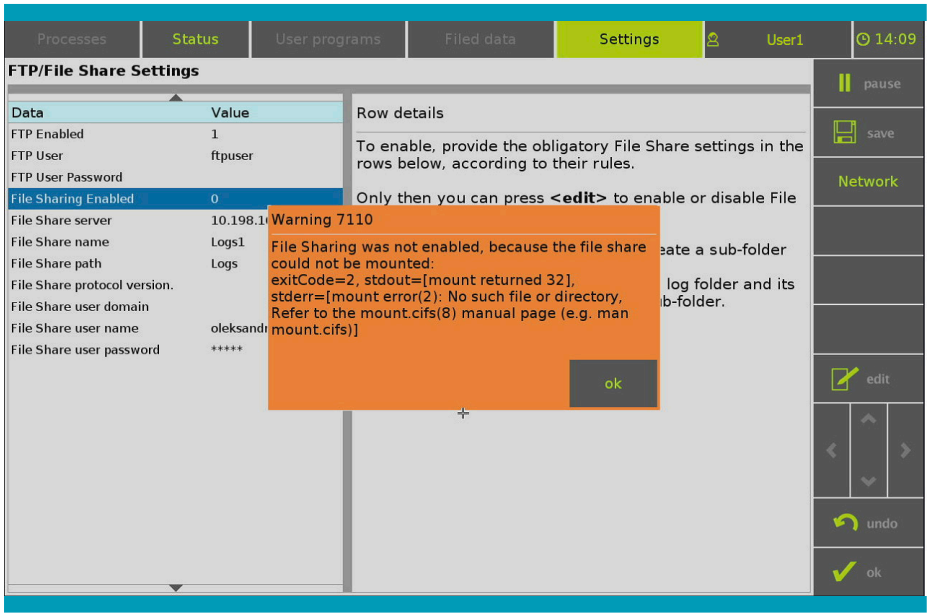
2. Para introducir el nombre de host o la dirección IP del servidor SMB, seleccionar <File Share server> y tocar <edit>.

3. Para introducir el nombre del recurso compartido, seleccionar <File Share name> y tocar <edit>.

4. (Opcional) Seleccionar <File Share path> y tocar <edit> para introducir la ruta. Si se introduce esta ruta, los archivos generados por el instrumento se enviarán a
\\[File Share server]\[File Share name]\[File Share path]\

   Si esta ruta está vacía, los archivos generados se enviarán a
\\[File Share server]\[File Share name]\
Si no se encuentra la carpeta, el software emitirá un aviso (Pantalla 9.5).

IMPORTANTE
Se recomienda no utilizar espacios en «File Share path».



Pantalla 9.5: Advertencia de fallo de la configuración del intercambio de archivos

5. Para introducir la versión del protocolo SMB, seleccionar <File Share protocol version> y tocar <edit>.

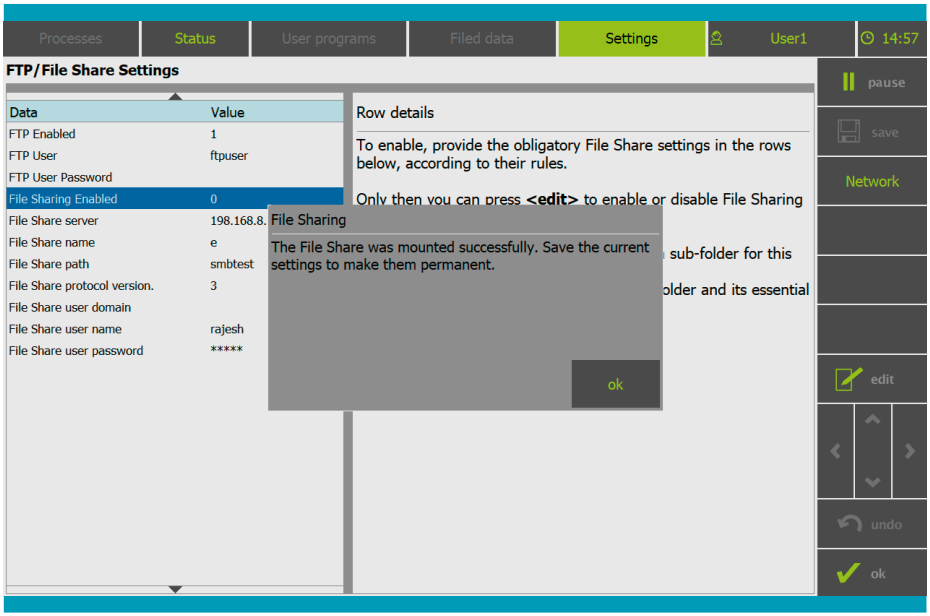
6. Para introducir el dominio del usuario, seleccionar <File Share user domain> y tocar <edit>. Repita los pasos para <File Share user name> y <File Share user password>.

IMPORTANTE

Si se utiliza el usuario «Guest» (Invitado) para compartir la carpeta de almacenamiento, File Share user domain, File Share username y File Share user password deben estar vacíos.

7. Ajustar <File Sharing Enabled> a 1.

Después de la configuración, una ventana emergente mostrará si la configuración es correcta (ver la Pantalla 9.6).



Pantalla 9.6: Configuración correcta para el intercambio de archivos

IMPORTANTE

La modificación de los parámetros de intercambio de archivos desactivará el intercambio y será necesario reactivarlos manualmente. Confirme siempre que esté habilitado «File Sharing Enabled» (valor ajustado a 1).

9.4 Configuración de la transferencia de archivos por FTP

FTP es un protocolo de red que permite la transferencia de datos entre el CliniMACS Prodigy (denominado servidor FTP) y el ordenador del usuario final (denominado cliente FTP) a través de conexiones IP (Internet Protocol, protocolo de Internet).

IMPORTANTE

- Asegurarse de que la conexión FTP solo se utilice en una red interna, sin acceso a o desde Internet. El usuario debe garantizar la seguridad de la red.
- Asegurarse de que los ajustes del cortafuegos del ordenador cliente estén configurados adecuadamente para conexiones FTP activas o pasivas, a fin de permitir el intercambio de datos con el instrumento.

Nota: Los datos accesibles del CliniMACS Prodigy a través de FTP son de solo lectura y únicamente se pueden descargar

Para conectar el cliente FTP al instrumento es necesario iniciar sesión.

El instrumento se debe configurar de forma diferente según la opción de inicio de sesión. Se admiten dos opciones de inicio de sesión:

- Opción de inicio de sesión 1: una cuenta registrada en el UMS. Asegurarse de que la función «File management user» esté asignada a esta cuenta. En este caso, el establecimiento y la finalización de la conexión se grabarán en el audit trail. Para más información relativa a funciones y la administración de usuarios, consultar el capítulo 10 ´Administración de usuarios´.
- Opción de inicio de sesión 2: un nombre de usuario local y una contraseña guardados en FTP/File Share Settings.

9.4.1 Configuración del instrumento

1. Ir a <FTP/File Share Settings>. Para FTP solo son relevantes los parámetros del cuadro azul.

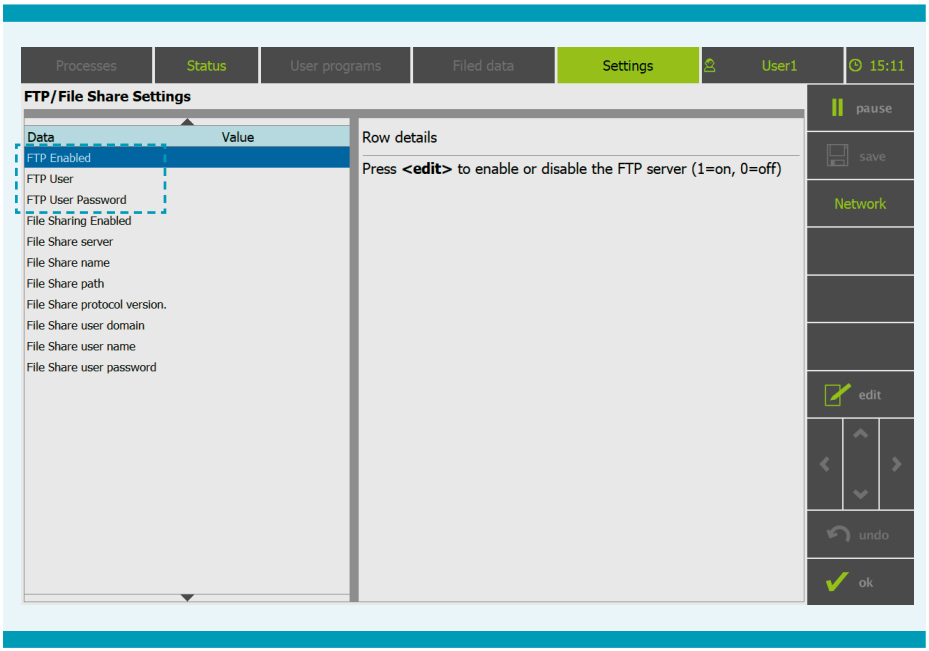


Figura 9.3: Parámetros de intercambio de archivos

2. (Omitir este paso, para la opción de inicio de sesión 1) para introducir el nombre de usuario al iniciar sesión desde el cliente FTP, ir a <FTP User> y tocar <edit>. No es necesario que el nombre de usuario utilizado para el cliente FTP esté registrado en el sistema de administración de usuarios. El nombre de usuario debe empezar por una letra y puede contener minúsculas, mayúsculas, números y guiones bajos.

   Nota: Si <FTP User> está ajustado a «N/A», la conexión FTP se desactivará.

3. (Omitir este paso, para la opción de inicio de sesión 1) Para introducir la contraseña, ir a <FTP User Password> y tocar <edit>. La contraseña debe contener al menos seis caracteres y puede constar de minúsculas, mayúsculas, números y los caracteres especiales +#!?=.
4. Para habilitar la conexión FTP, ir a <FTP Enabled> y ajustar el valor del campo de entrada a 1.
5. Para guardar los ajustes, tocar <ok> en la barra de herramientas.

9.4.2 Conexión con el cliente FTP

El usuario se puede conectar al instrumento con cualquier cliente FTP disponible (p. ej., FileZilla) para descargar protocolos y archivos de registro después de la configuración. Para conectarse al instrumento, introducir los datos siguientes:

- La dirección IP del instrumento. Figura en <Settings> ▸ <Tools> ▸ <Info> ▸ <Network information>.
- El puerto: use el puerto predeterminado 21.
- Nombre de usuario y contraseña: para la opción de inicio de sesión 1: introducir el ID de cuenta y la contraseña registrados en la administración de usuarios. Para la opción de inicio de sesión 2: introducir el nombre de usuario y la contraseña como se describe en los pasos 2 y 3.

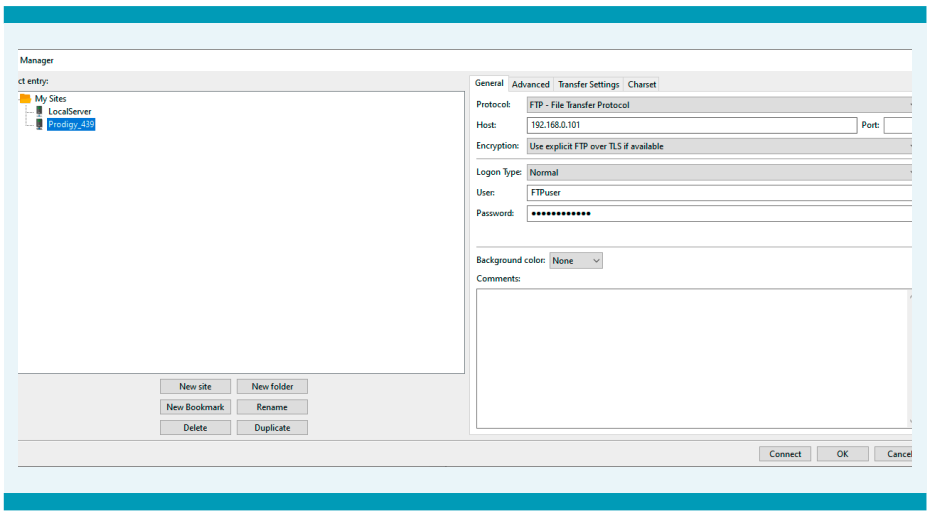


Figura 9.4: Ejemplos de parámetros de conexión

Nota: Un usuario individual solo podrá establecer una única conexión a la vez, ya que el servidor del instrumento no permite conexiones múltiples. Si se emplea un software cliente que utiliza conexiones simultáneas (p. ej., FileZilla), cambie los

ajustes del cliente en consecuencia para permitir una sola sesión. De lo contrario, los contenidos solo se podrán examinar, pero no descargar.

9.5 Conexión a un servidor de correo electrónico

El software puede enviar un correo electrónico a una dirección electrónica previamente introducida en caso de error o mensajes de advertencia durante la ejecución de un proceso. El correo electrónico contendrá mensajes de advertencia/error y una captura de pantalla del instrumento (ver la Figura 9.5). La notificación por correo electrónico es compatible con los protocolos Simple Mail Transfer Protocol (SMTP) y Simple Mail Transfer Protocol Secure (SMTPS).

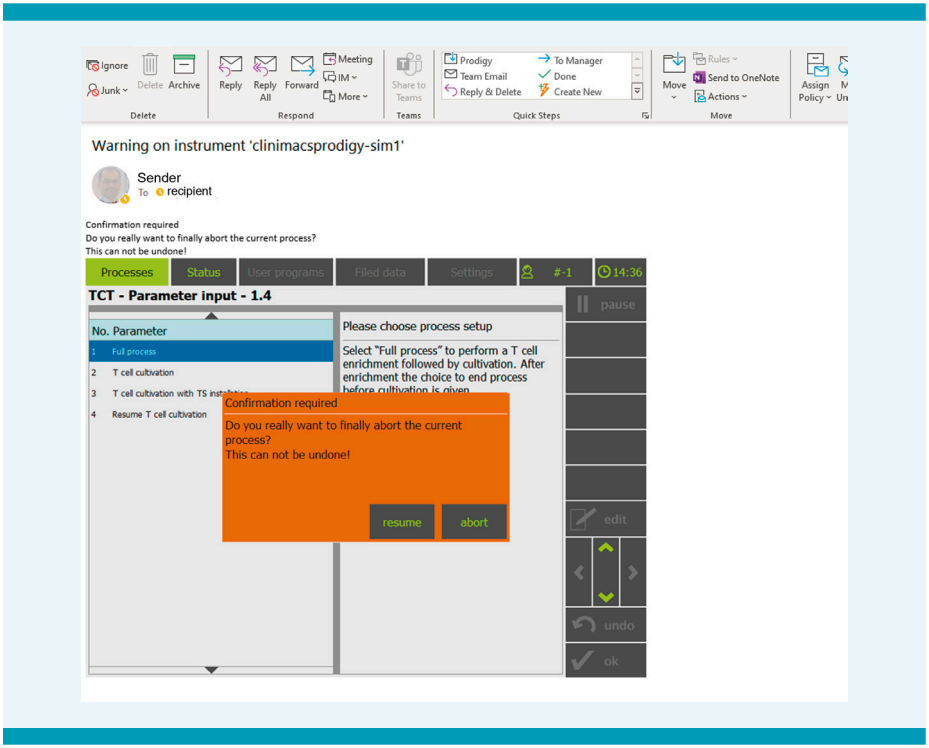


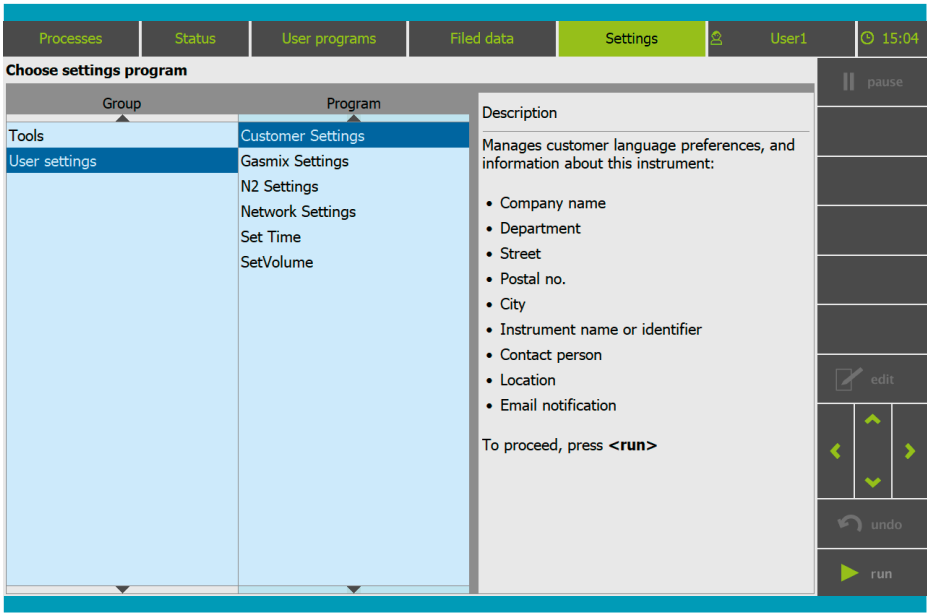
Figura 9.5: Ejemplo de un correo electrónico

Requisitos:

- Un servidor de correo electrónico compatible con el protocolo SMTP o SMTPS. Asegurarse de que este servidor sea accesible. Anote la dirección IP y el puerto del servidor.
- Una cuenta de correo electrónico de cliente creada previamente que se puede utilizar para la autenticación durante la configuración.
- El instrumento está conectado a Ethernet y la red está habilitada.

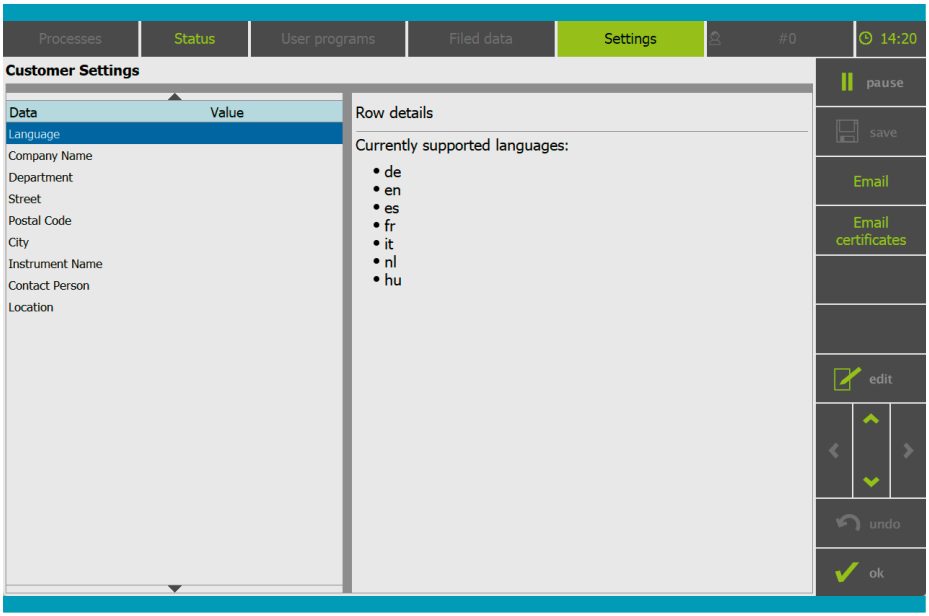
Configuración del instrumento:

1. Para introducir los ajustes personalizados, ir a <Settings> ▸ <User settings> ▸ <Customer Settings> y tocar <run> (ver la Pantalla 9.7).



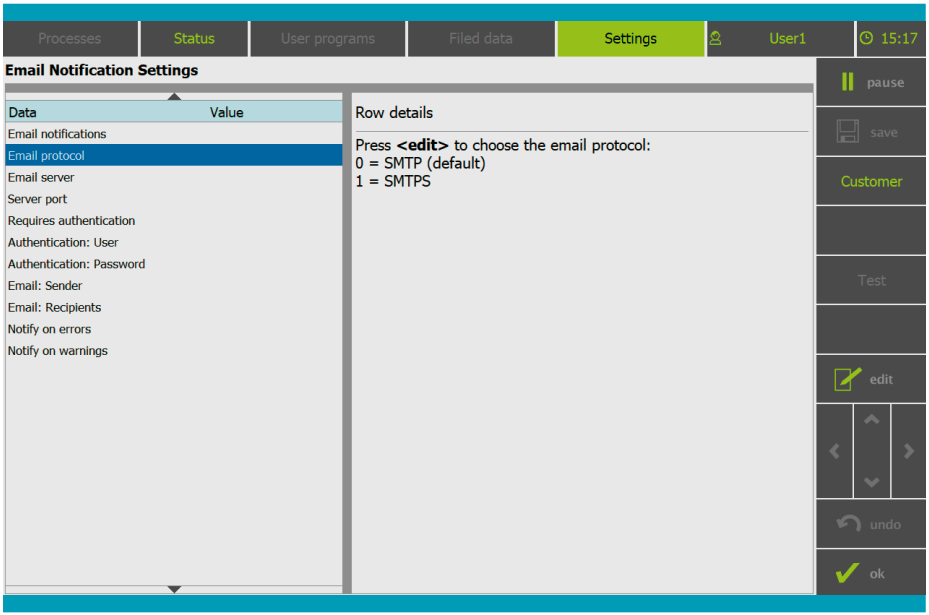
Pantalla 9.7: Inicio de los ajustes personalizados

2. Para acceder a <Email Notification Settings>, tocar <Email> en la barra de herramientas (ver la Pantalla 9.8).



Pantalla 9.8: Ajustes de correo electrónico

3. Para introducir el valor correspondiente al protocolo utilizado por el servidor de correo electrónico, ir a <Email protocol> y tocar <edit>. Por defecto está seleccionado SMTP(0).



Pantalla 9.9: Parámetros para la notificación por correo electrónico

4. Para introducir el nombre de host o la dirección IP del servidor de correo electrónico, ir a <Email server>.

5. Para introducir el puerto utilizado en el servidor de correo electrónico, ir a <Server port> y tocar <edit>.

Si se utiliza el puerto predeterminado, no es necesario editar este campo.

Protocolo	Puerto predeterminado	Puerto alternativo
SMTP	25	2525, 465, 587
SMTPS	465	587 (TLS)

Tabla 9.1: Puerto para el servidor de correo electrónico

6. Seleccionar <Requires authentication>. Si el servidor de correo electrónico solicita autenticación, ajustar este campo a 1 e introducir el nombre de usuario y la contraseña de autenticación como se describe en el paso 7; de lo contrario, ir al paso 9.

7. Para introducir el nombre de usuario y la contraseña, ir a <Authentication: User> y <Authentication: Password>. **Nota:** Una cuenta de autenticación la pueden compartir varios instrumentos. Consultar a su departamento informático si necesita ayuda.

8. Para introducir la dirección de correo electrónico del remitente, ir a <Email: Sender> y tocar <edit>. El <Email: Sender> puede ser idéntico al usuario de autenticación.

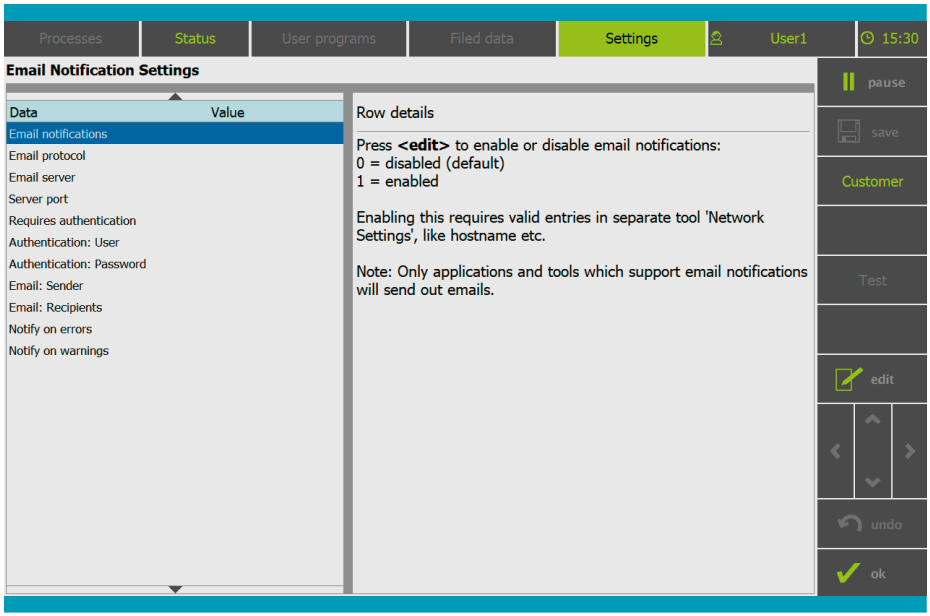
9. Para introducir las direccione electrónicas de los destinatarios, ir a <Email: Recipients> y tocar <edit>. Los destinatarios también pueden ser una dirección electrónica de grupo.

Nota: Se pueden introducir varios destinatarios, separados por un espacio.

10. Si desea recibir mensajes de error, ir a <Notify on errors> y tocar <edit>. Ajustar el valor a 1 para activar los mensajes. Por defecto, la función <Notify on errors> está desactivada (valor ajustado a 0).

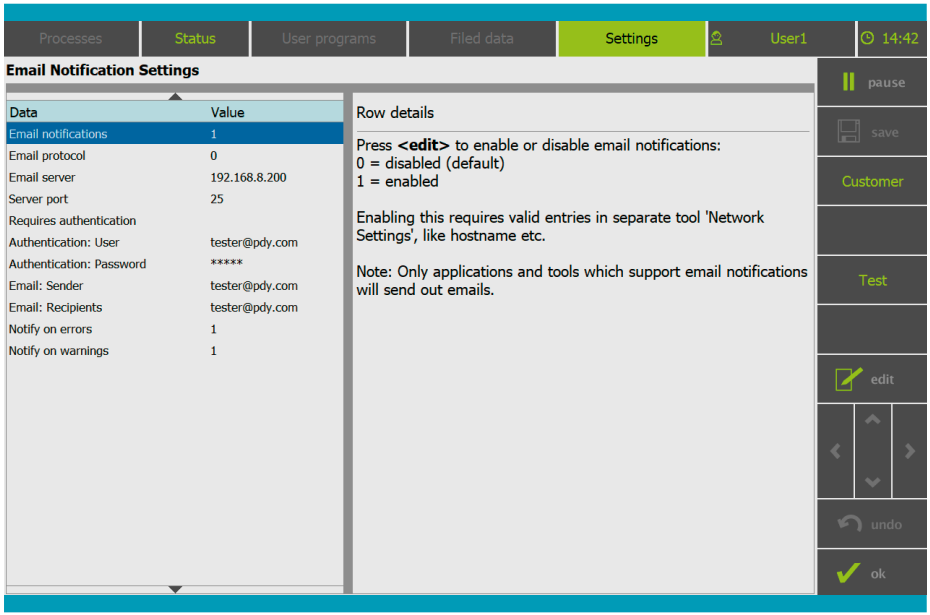
11. Si desea recibir mensajes de advertencia, ir a <Notify on warnings> y tocar <edit>. Ajustar el valor a 1 para activar los mensajes. Por defecto, la función <Notify on warnings> está desactivada (valor ajustado a 0).

12. Para activar las notificaciones por correo electrónico, ir a <Email notifications> y tocar <edit> (ver la Pantalla 9.10). Ajustar el valor a 1 para activar las notificaciones. Por defecto, las notificaciones por correo electrónico están desactivadas (valor ajustado a 0).



Pantalla 9.10: Activación de la notificación por correo electrónico

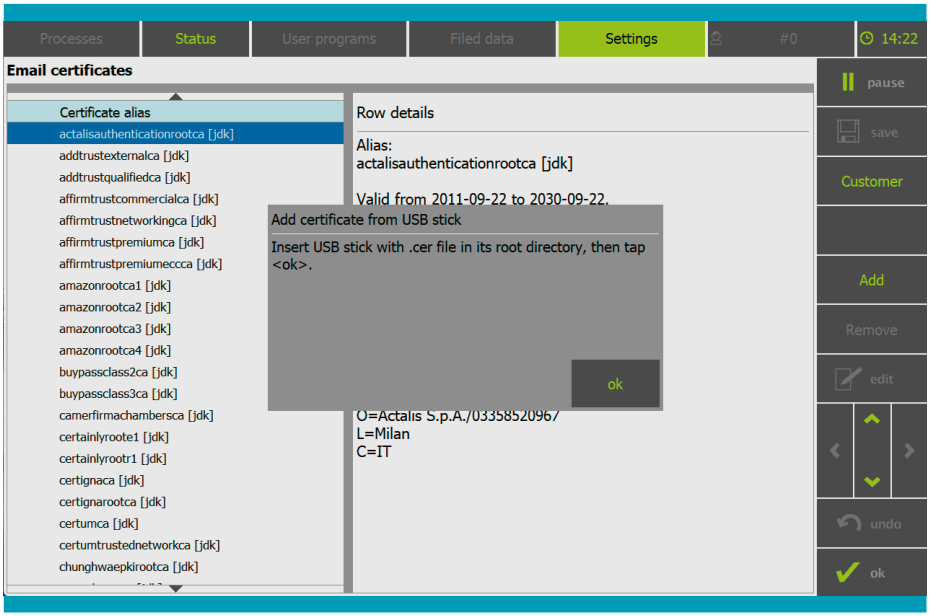
13. Una vez introducidos todos los datos necesarios, se activará el botón <Test> de la barra de herramientas. Para enviar un correo electrónico de prueba, tocar <Test> en la barra de herramientas.



Pantalla 9.11: Envío de un correo electrónico de prueba

Certificados de correo electrónico

Algunos de los certificados más comunes ya están disponibles en el instrumento. Si se necesitan certificados adicionales, deberán cargarse.



Pantalla 9.12: Añadir certificado desde una memoria USB

Para añadir un nuevo certificado, pulsar < Add > y seguir las instrucciones que aparecen en pantalla.

9.6 Activación de la sincronización horaria de la red

NTP es un protocolo de red que permite la sincronización del reloj y la gestión centralizada del tiempo.

Solo los usuarios del UMS con la función de administrador «Administration tools user» o un usuario con la función «network setting tools user» podrán acceder a la configuración de red. Para activar la funcionalidad NTP en el instrumento, seguir estos pasos:

1. Ir a <Settings> ▸ <User Settings> ▸ <Network Settings> y tocar <run>. Aparecerá la configuración de red. Los parámetros del cuadro azul son relevantes para la sincronización horaria de la red (ver la Figura 9.6).

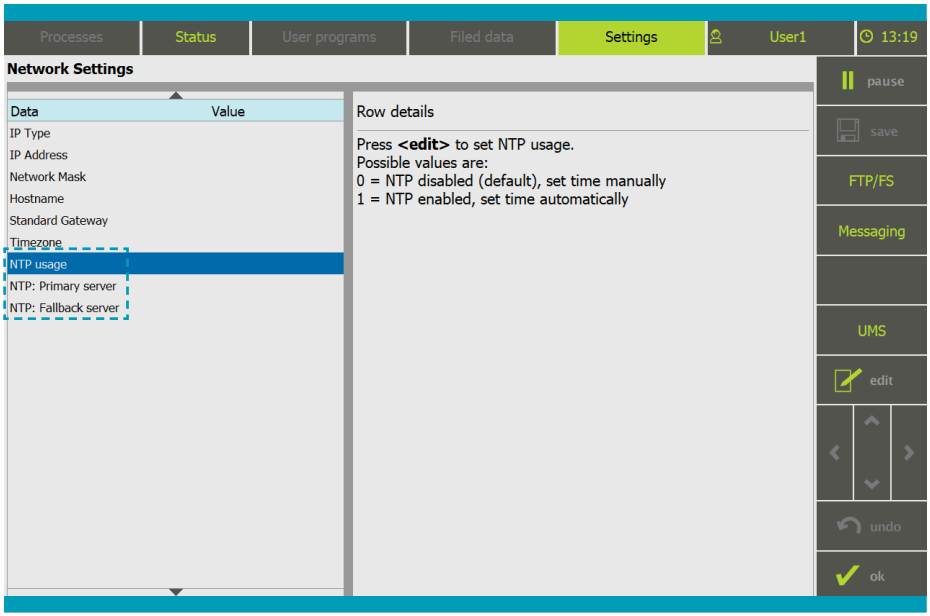


Figura 9.6: Configuración de NTP

2. Para activar NTP y ajustar la hora automáticamente, tocar <NTP usage> y ajustar el valor a 1, después tocar <ok> en el campo de entrada.
3. Para introducir el nombre de host/la dirección IP, tocar <NTP: Primary server> o <NTP: Fallback server> y después <edit>. Para confirmar la entrada, tocar <ok>.
4. Tocar <Save> y confirme que estos cambios se deben aceptar y guardar. La configuración del servidor NTP está activada.
5. Reinicie el sistema (ver la sección 8.7 «Apagado»).

10 Administración de usuarios

10.1 Información general

El sistema de administración de usuarios del software admite la autenticación de usuarios y el control de acceso basado en funciones para respaldar el cumplimiento de la norma 21 CFR Parte 11.

- Autenticación del usuario: se requiere un nombre de usuario (también denominado ID de cuenta) y una contraseña para iniciar sesión y utilizar el instrumento. Se admite tanto la administración local de usuarios como la autenticación LDAP.
- Control de acceso basado en funciones: los usuarios con diferentes funciones tienen distintos derechos de acceso. En el control de acceso basado en funciones se definen tres términos: derechos, funciones y cuentas.

Derechos

Los derechos representan la unidad mínima asignable de acciones de usuarios. Los derechos se definen por el software y el usuario solo puede agrupar los derechos existentes. Para un resumen de los distintos derechos del programa, ver la Tabla A.1 en el Anexo.

Funciones

Las funciones representan cargos o responsabilidades laborales dentro de una organización. A una función se puede asignar un conjunto de derechos. El software proporciona funciones predeterminadas. Las funciones importantes predeterminadas se enumeran en la Tabla 10.1. El software admite funciones personalizadas.

Cuentas

Las cuentas representan a usuarios individuales. En un entorno GMP debe existir una relación unívoca entre el ID de una persona y el ID de una cuenta. Tras la instalación se creará una cuenta de administrador con todas las funciones. Esto permitirá al usuario crear nuevas funciones y nuevas cuentas en caso necesario.

Función	Herramientas/derechos
Application x.x operator (Operario de aplicación x.x)	Permiso para ejecutar esta aplicación con el número de versión x.x
ATS user (Usuario ATS)	Acceso a audit trail, incluidas la visualización, exportación y eliminación
Administration tools user (Usuario de herramientas de administración)	Acceso a herramientas para administrar el instrumento. Propuesto para administradores
Common tools user (Usuario de herramientas comunes)	Acceso a herramientas comunes: Info, License, Shutdown y User Settings. Propuesto para todos los usuarios
File management user (Usuario de administración de archivos)	Acceso a la herramienta Backup Filed Data y a la herramienta Custom Files. Habilita el acceso al archivo de registro a través de FTP
Gas mix tool v1.0 Operator (Operario de la herramienta de mezcla de gases v1.0)	Acceso a la herramienta de mezcla de gases
Injected programs (Programas inyectados)	Permiso para ejecutar programas inyectados
Acceso a la herramienta N_2 settings (ajustes N_2)	Acceso a la herramienta de ajuste para N_2
Set time user (Usuario de ajuste de la hora)	Permite ajustar la hora
Support tools user (Usuario de herramientas de apoyo)	Chamber in, Chamber out, Sealer e Instrument check
UM Administrator	Acceso a la administración de usuarios que permite administrar las cuentas
UM user	Operador definido que iniciará y ejecutará las aplicaciones de usuario

Tabla 10.1: Resumen de las funciones predeterminadas

A continuación se muestra un ejemplo de una configuración del UMS convencional:

- Un administrador gestiona las cuentas y el instrumento. La función de administrador suele permitir la configuración y el cambio de cuentas, y proporciona acceso a la administración de archivos y a herramientas avanzadas para la configuración de instrumentos.

- Un operario inicia y ejecuta aplicaciones en el instrumento. La cuenta de operario se configuraría para permitir la ejecución de un conjunto concreto de aplicaciones y herramientas en función de las decisiones de administración de usuarios del cliente para prestar asistencia y solucionar problemas. Puede haber más de un tipo de usuario definido por el cliente y a cada usuario se le puede asignar una o más funciones.

IMPORTANTE

Para un operario se deberá asignar la función «UM User». Para un administrador se deberá asignar la función «UM Administrator».

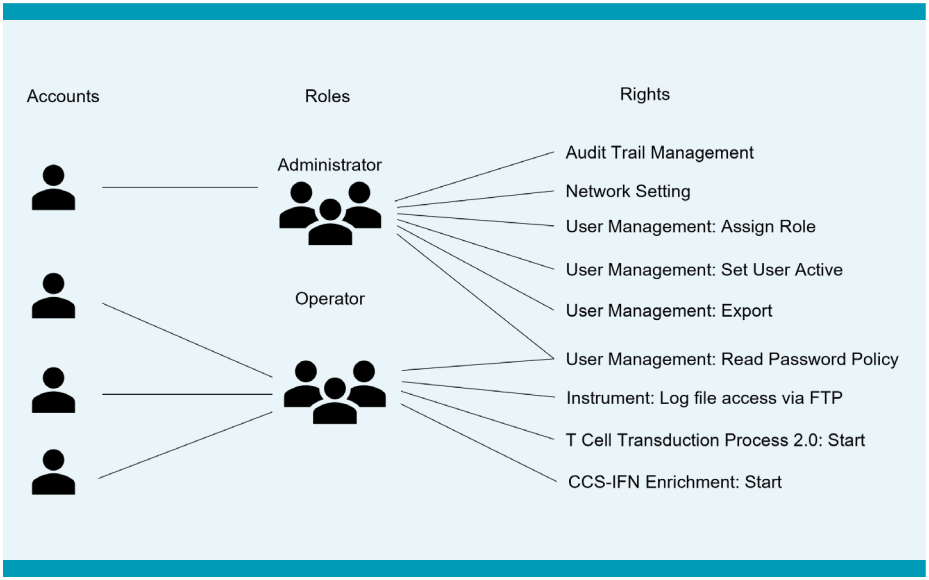


Figura 10.1: Ejemplos de parámetros de conexión

⚠ ATENCIÓN

Riesgo de fracaso del proceso por un inicio de sesión fallido. Si ya no fuera posible iniciar sesión, existe el riesgo de que el proceso fracase. Para evitar esta situación, se deberán crear cuentas de usuario y de administrador adecuadas con contraseñas distintas antes de iniciar una aplicación en el instrumento. Si ya no fuera posible iniciar sesión en un instrumento, póngase en contacto con Miltenyi Biotec Technical Support.

IMPORTANTE

- Se recomienda encarecidamente establecer una solución de emergencia para situaciones de emergencia Podría tratarse de una cuenta de administrador adicional para uso de emergencia. Las credenciales de la cuenta de emergencia se deberán guardar en un lugar seguro y solo estarán disponibles para determinadas personas.
- El procedimiento de autenticación se deberá describir y aplicar dentro del

sistema de gestión de la calidad del centro, y todos los usuarios y administradores deberán recibir la formación correspondiente.

- Si fallara la conexión LDAP, utilice una cuenta de usuario local para acceder al instrumento.

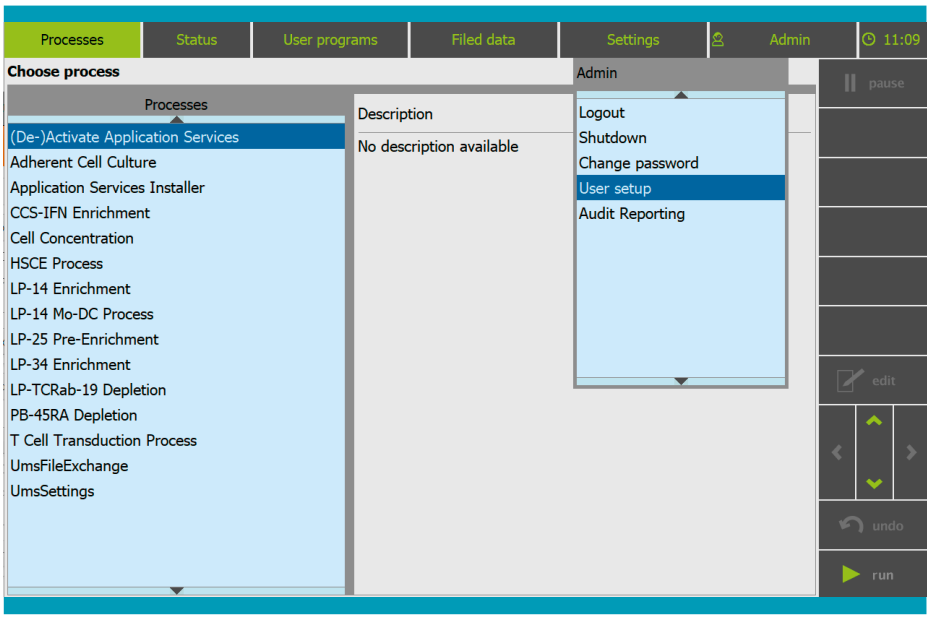
10.2 Administrar funciones y cuentas

IMPORTANTE

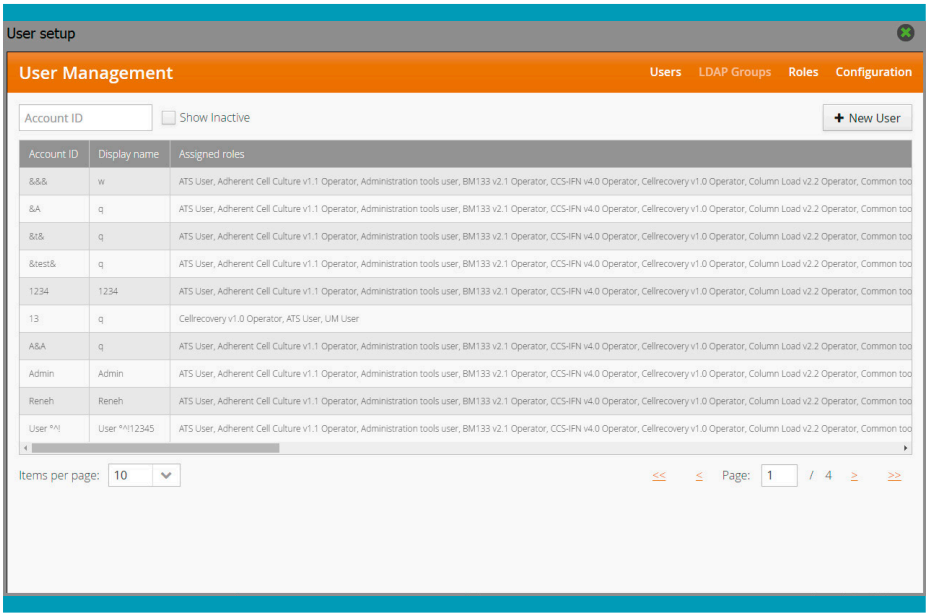
Un usuario debe tener la función «UM Administrator» para configurar el sistema de administración de usuarios.

10.2.1 Acceso a la administración de usuarios

Para acceder al sistema de administración de usuarios ir a (menú de acceso rápido) y tocar <User setup>. Se mostrará la página de administración de usuarios (Pantalla 10.2). La administración de usuarios tiene cuatro páginas: <Users>, <LDAP Groups>, <Roles> y <Configuration>. Por defecto está seleccionado <Users>.



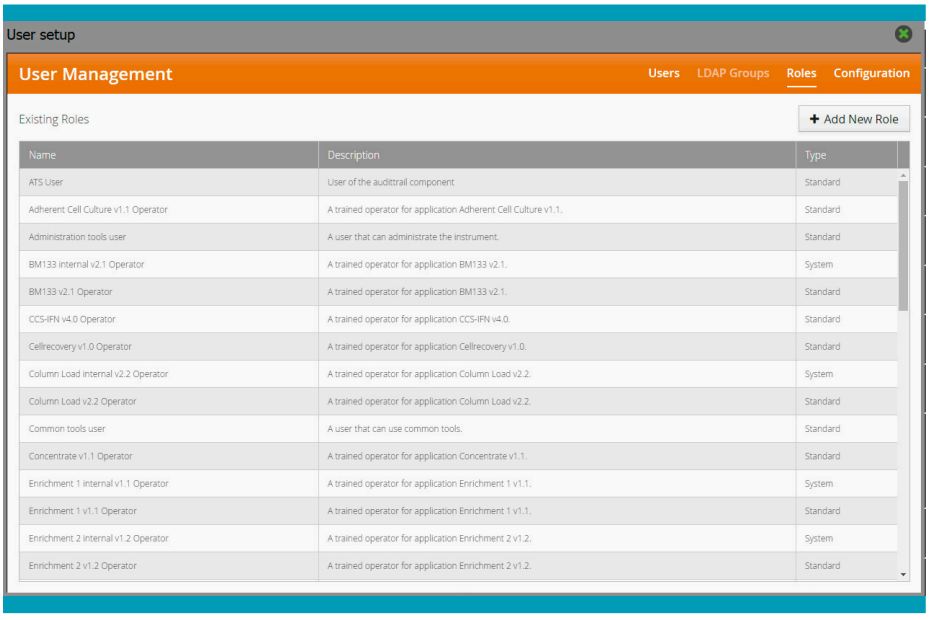
Pantalla 10.1: Selección de User setup (Configuración de usuario)



Pantalla 10.2: Menú User Management

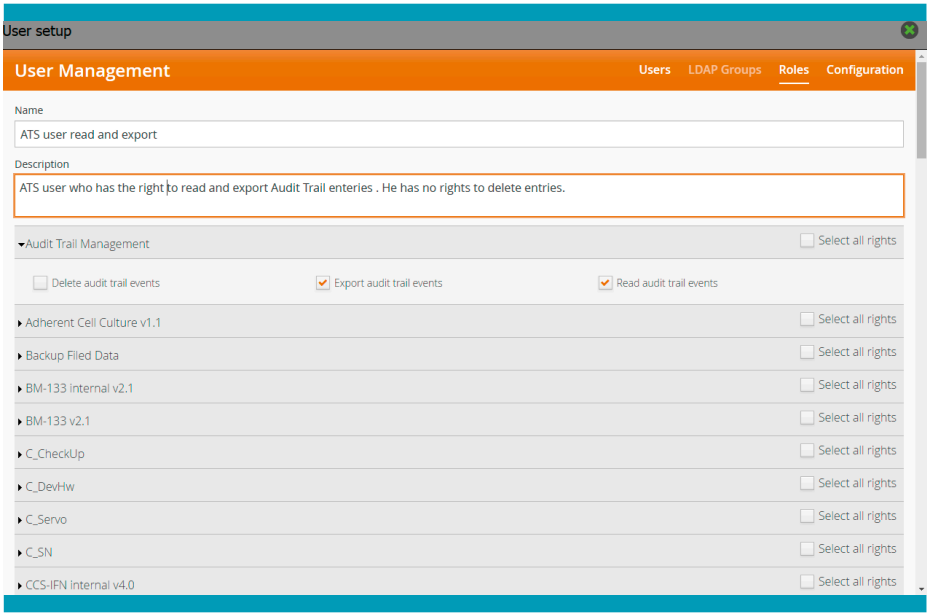
10.2.2 Crear una nueva función

1. Tocar <Roles> en <User Management>. Se mostrará una lista de las funciones existentes (Pantalla 10.3).



Pantalla 10.3: Funciones definidas en la administración de usuarios

2. Tocar <+Add New Role> (Pantalla 10.3). Se mostrará una nueva página de definición de funciones (ver la Pantalla 10.4).



Pantalla 10.4: Crear una nueva función

3. Introducir el nombre y la descripción de la función. Marque el derecho deseado para esta función.
4. Tocar <Save> en la parte inferior de la página. La nueva función agregada se muestra en la lista de funciones existentes y se puede asignar a un usuario.

10.2.3 Cambiar los derechos de las funciones

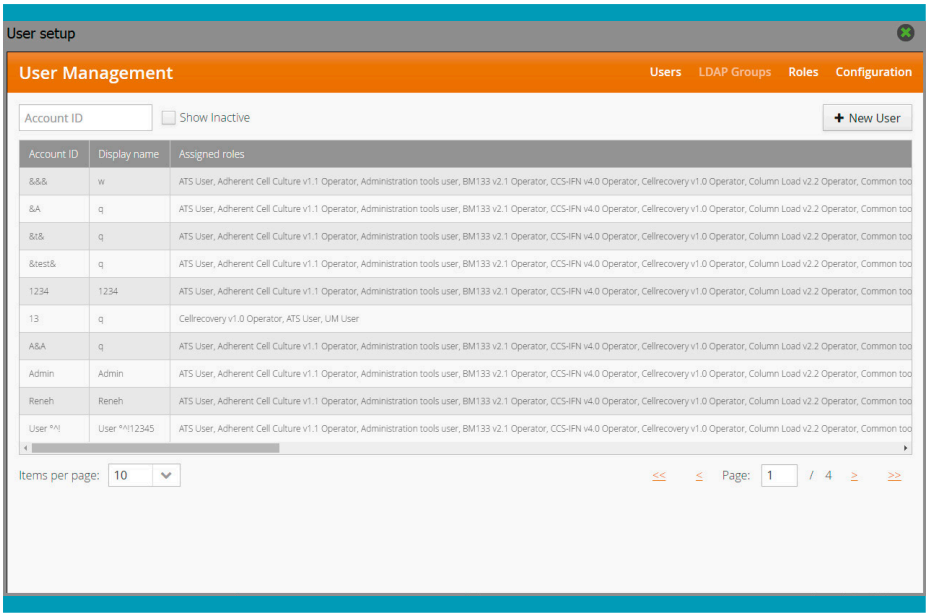
1. Localizar y seleccionar la función en la lista de funciones existentes (ver la Pantalla 10.3)
2. Seleccionar o anule la selección de los derechos deseados.
3. Desplacerse a la parte inferior y tocar <Save>.

10.2.4 Agregar un usuario local

IMPORTANTE

- Un usuario debe tener la función «UM Administrator» para crear una nueva cuenta.
- En un entorno GMP se deberán utilizar nombres reales o sinónimos que se puedan distinguir y reconocer claramente.

1. Seleccionar el menú <Users> en la administración de usuarios.
2. Tocar <+New User>. Se mostrará una nueva página de usuarios (Pantalla 10.5).

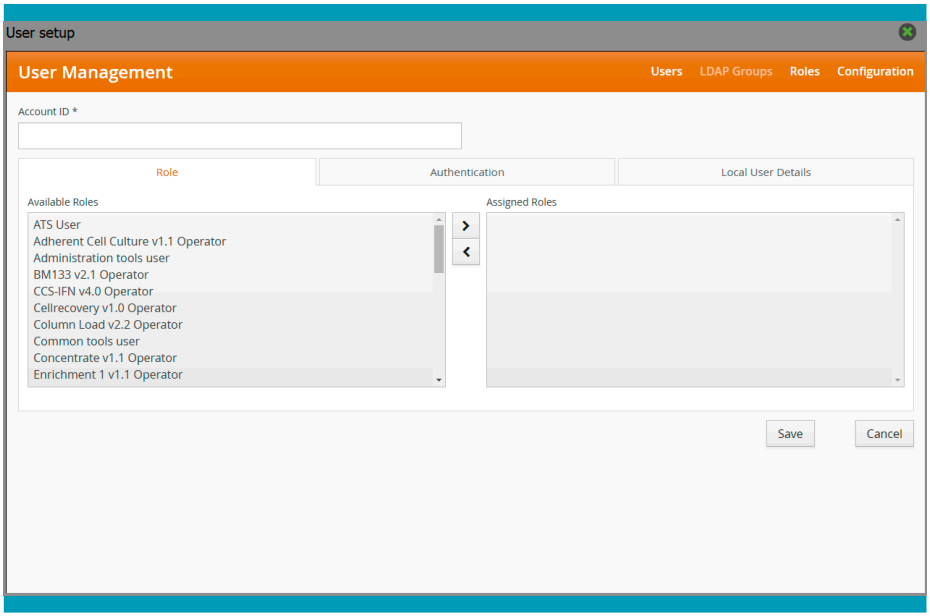


Pantalla 10.5: Menú «New User»

3. Introducir el ID de cuenta (Pantalla 10.6). Este ID de cuenta debe ser único y tener una relación unívoca con los usuarios finales. El ID de cuenta corresponde al nombre de usuario al iniciar sesión.

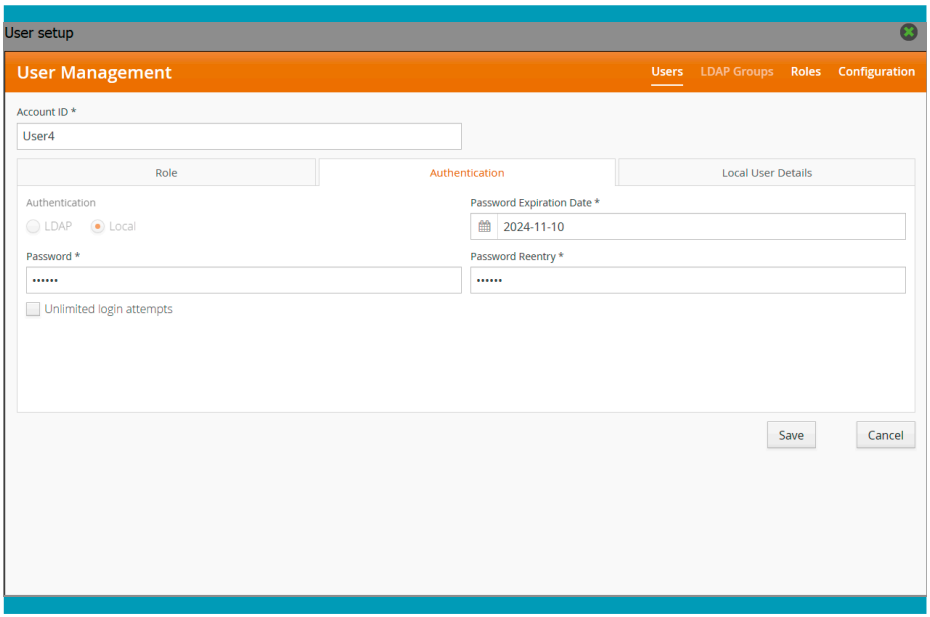
   Si está configurado Active Directory, el software comprobará si este ID está registrado en el servidor AD. Si no se localiza el ID, se creará una cuenta local. Si se localiza el ID, se utilizará por defecto la cuenta AD. Para cambiar una cuenta LDAP a una cuenta local, seguir el paso 5.

4. Para asignar las funciones correspondientes a esta cuenta, seleccionar la entrada en <Available Roles>, en la pestaña <Role> y tocar ⊡ (Pantalla 10.6). Para eliminar una función asignada a esta cuenta, seleccionar la entrada en <Assigned Roles> y tocar ⊡.



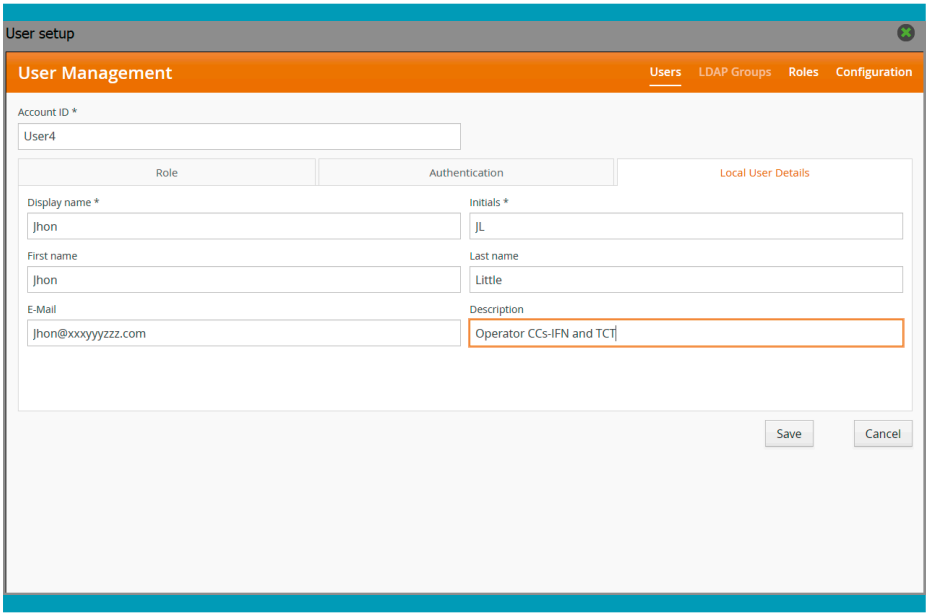
Pantalla 10.6: Página de configuración del usuario

5. Si está configurado LDAP y el ID de cuenta se localiza en el servidor AD, el usuario puede elegir entre la autenticación a través del servidor AD o de la base de datos local. Para un usuario local, introducir la contraseña y ajustar la fecha de caducidad, según la política de contraseñas (ver la sección 10.3 «Configurar la política de contraseñas»).



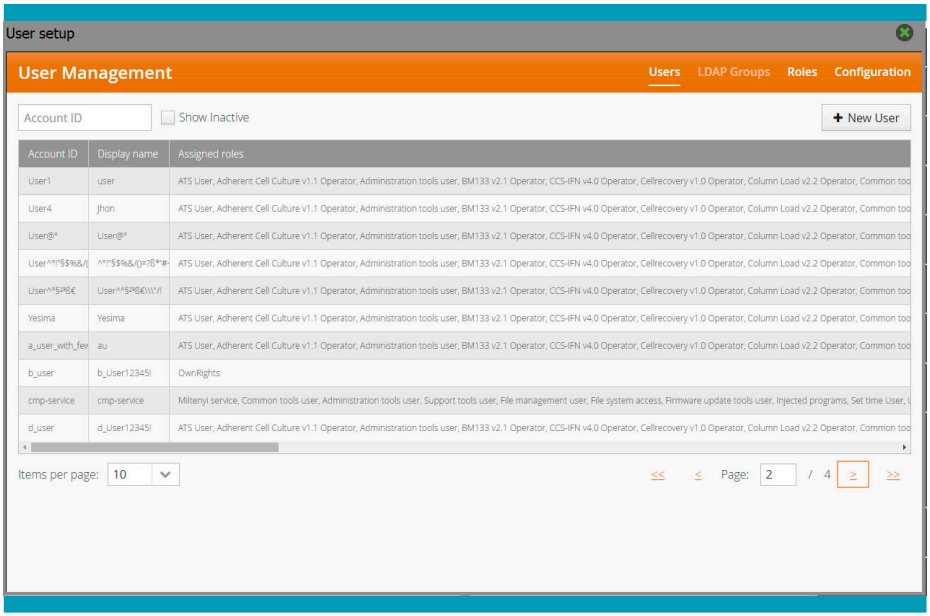
Pantalla 10.7: Introducción de la contraseña del nuevo usuario

6. En la pestaña <Local User Details>, ajustar información más detallada sobre esta cuenta.



Pantalla 10.8: Introducción de los datos del usuario local

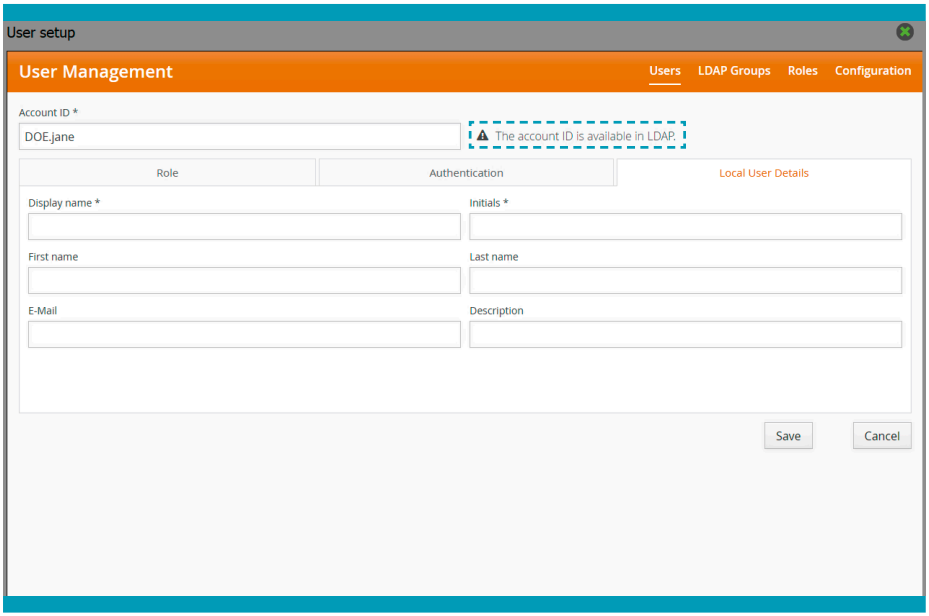
7. Tocar <Save>. La nueva cuenta agregada aparecerá en la lista de cuentas (Pantalla 10.9).



Pantalla 10.9: Confirmación del nuevo usuario agregado

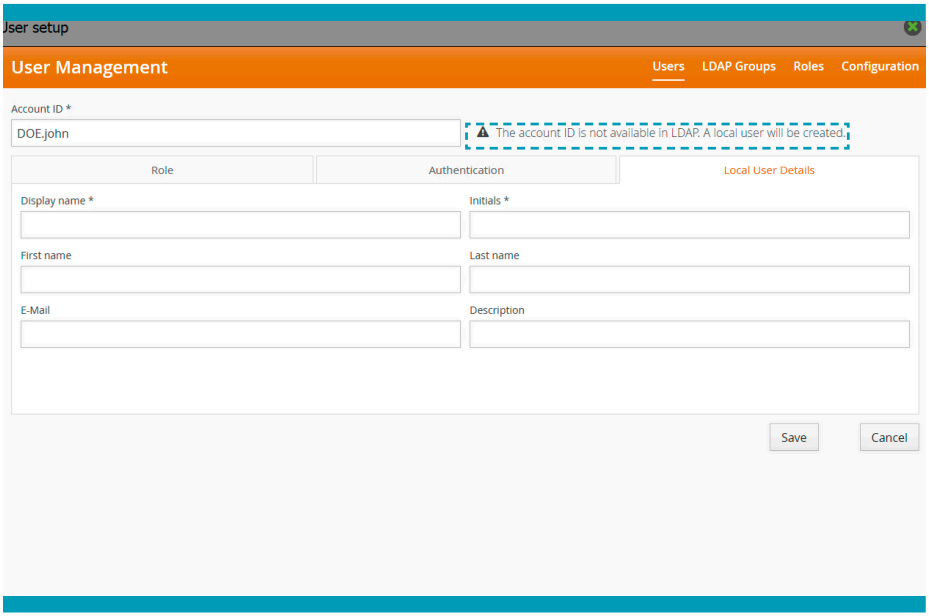
10.2.5 Agregar usuarios LDAP

1. Ir a **<Users>** en **<User Management>**.
2. Tocar **<+New User>**.
3. Introducir el ID de cuenta LDAP. El software comprobará si este ID está registrado en el servidor AD. Si el usuario ya existe, se rellenará más información utilizando la asignación de atributos (ver la Pantalla 10.10). Si el usuario no está registrado en AD, se creará un nuevo usuario local (ver la Pantalla 10.11).



Pantalla 10.10: Menú User Management de usuarios LDAP que muestra a modo de ejemplo un usuario registrado

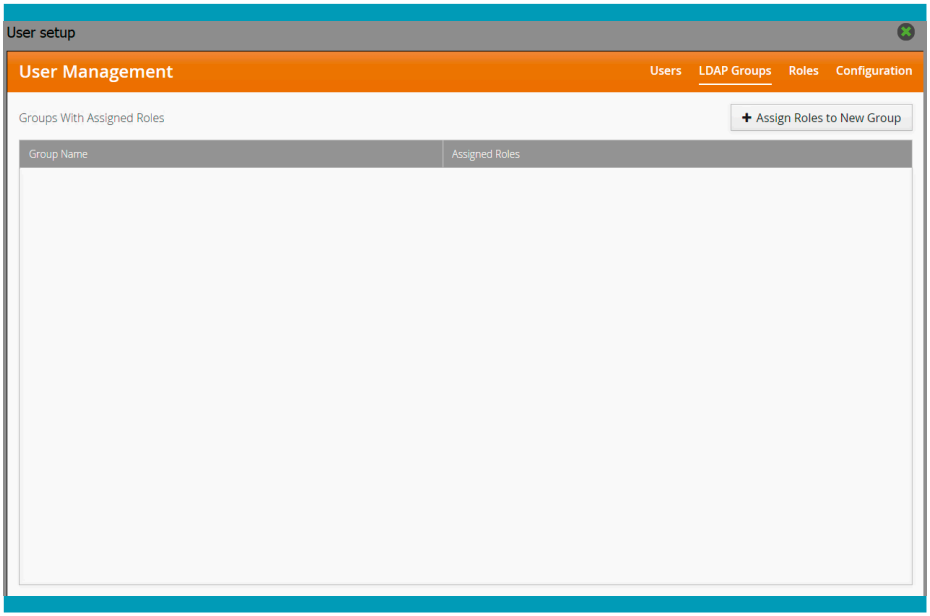
4. Para asignar funciones, tocar <Role> y seleccionar la función deseada.
5. Tocar <Save>. El usuario puede utilizar el ID de cuenta LDAP y la contraseña para iniciar sesión.



Pantalla 10.11: Menú User Management de usuarios LDAP que muestra a modo de ejemplo un usuario no registrado

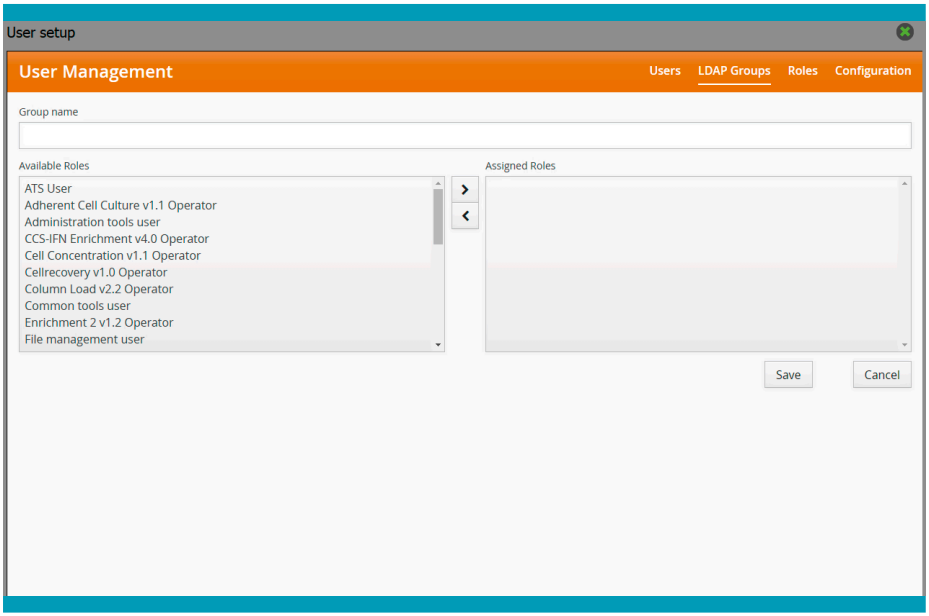
10.2.6 Agregar grupos LDAP

1. Seleccionar <LDAP Groups> en la barra de menús y tocar <+ Assign Roles to New Group>.



Pantalla 10.12: Menú User Management y paso necesario para agregar grupos LDAP

2. Introducir el nombre del grupo (ver la Pantalla 10.13). El sistema comprobará automáticamente si este grupo existe en LDAP.
3. Para asignar funciones a este grupo, seleccionar las funciones en <Available Roles> y tocar ›. Para eliminar una función asignada a un grupo, seleccionar la entrada en <Assigned Roles> y tocar ‹.
4. Tocar <Save>.



Pantalla 10.13: Menú User Management de grupos de usuarios LDAP

IMPORTANTE

Asegurarse de agregar el «UM Administrator» o el «UM User» correctos para garantizar un inicio de sesión adecuado.

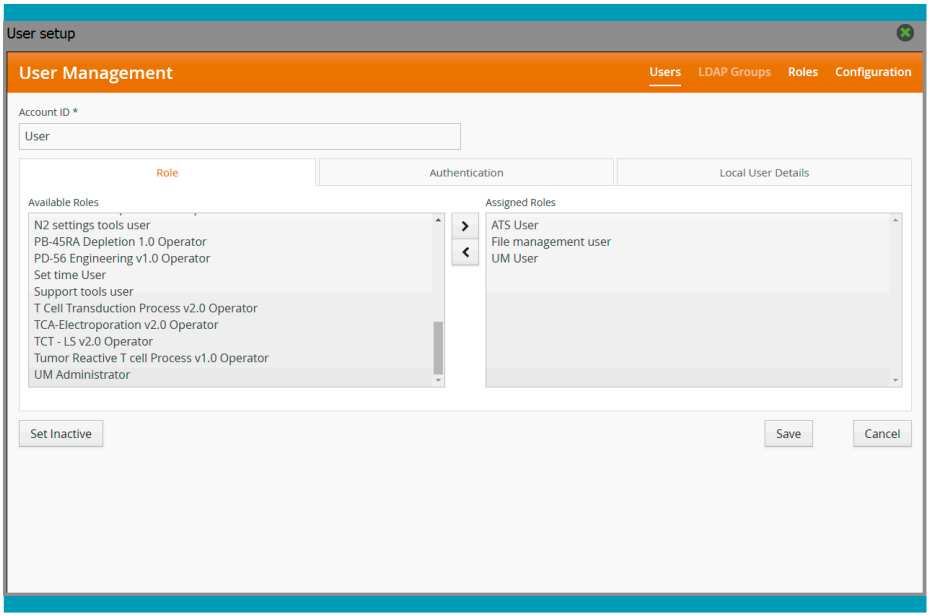
10.2.7 Cambiar las funciones asignadas a un usuario o grupo LDAP

1. Seleccionar el usuario en la lista de usuarios de la página de usuarios (Pantalla 10.2) y tocar el elemento deseado. Para el grupo LDAP, seleccionar el grupo deseado en la página de grupos LDAP (Pantalla 10.12).
2. Para asignar funciones adicionales al usuario, seleccionar la entrada en <Available Roles>, en la pestaña <Role> y tocar ›. Para eliminar funciones asignadas a esta cuenta, seleccionar la entrada en <Assigned Roles> y tocar ‹.
3. Tocar <Save> en la parte inferior de la pestaña <Role>.

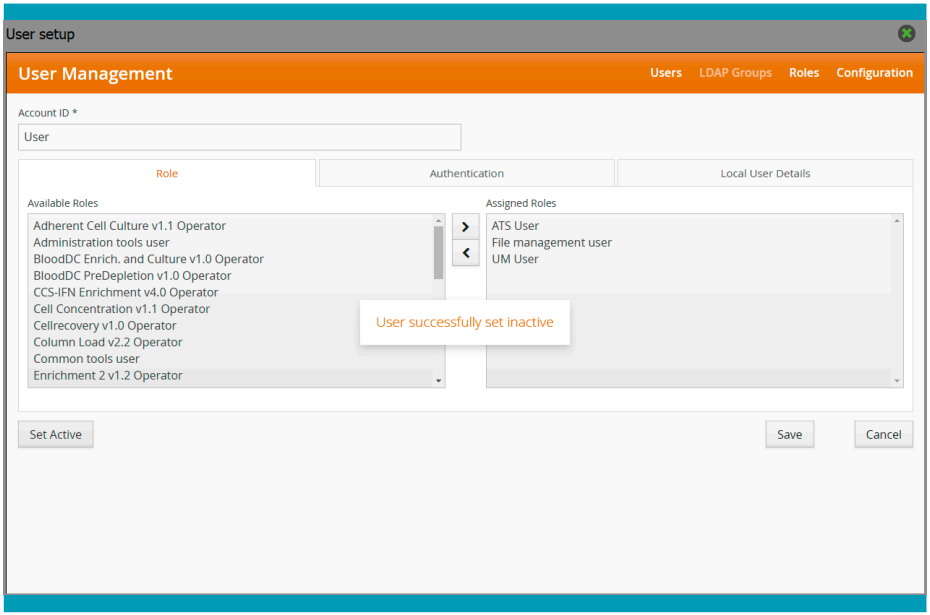
10.2.8 Desactivar usuarios locales

Nota: El usuario local no se puede eliminar, solo se puede desactivar.

1. Seleccionar el usuario local de la lista de usuarios (Pantalla 10.9). Se abrirá la página de configuración de usuarios.
2. Tocar <Set Inactive> en la parte inferior de la página de configuración de usuarios (Pantalla 10.14).

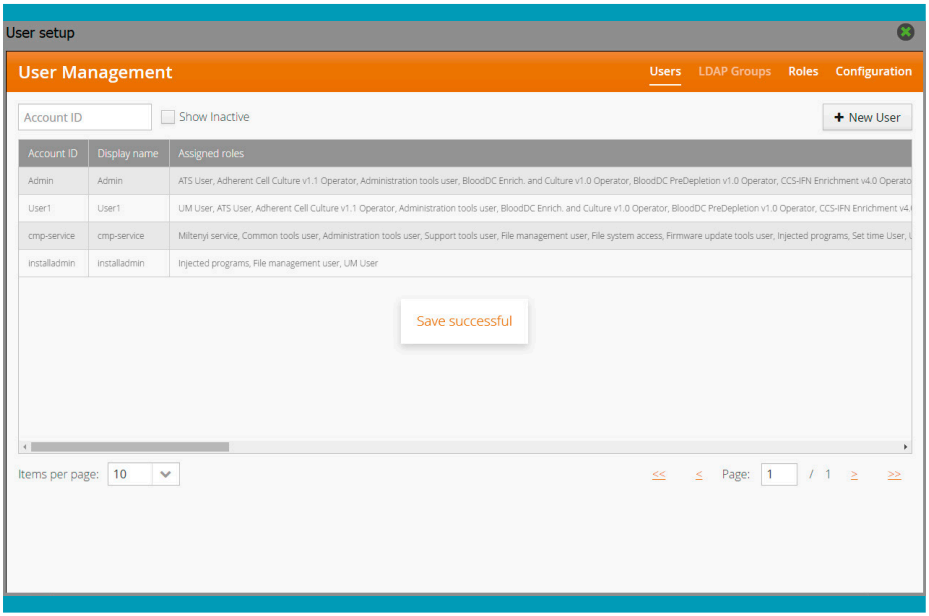


Pantalla 10.14: Ajuste de un usuario local a inactivo



Pantalla 10.15: Usuario correctamente ajustado a inactivo

3. Tocar <Save> en la parte inferior para volver a la lista de usuarios.

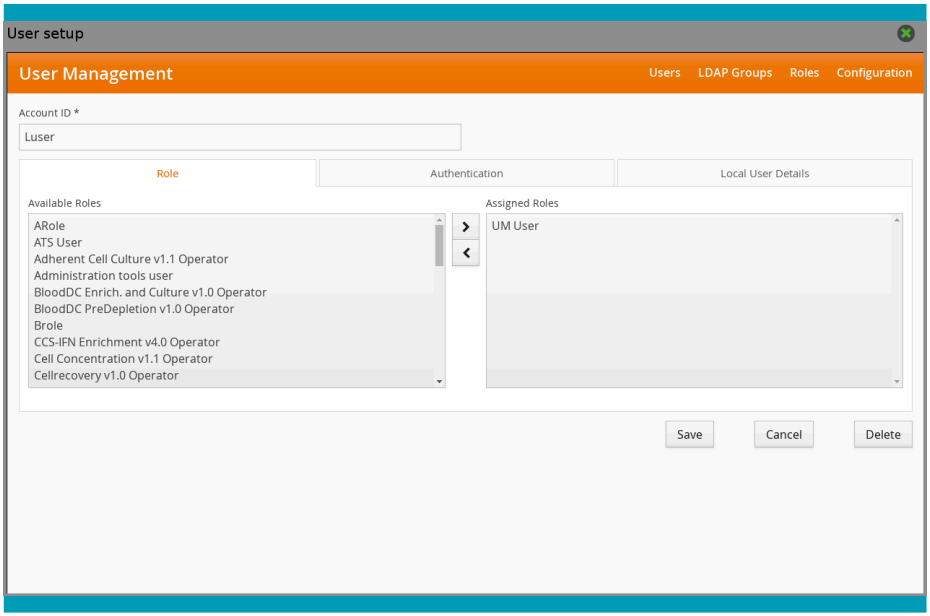


Pantalla 10.16: Guardado correcto

La cuenta inactiva no se mostrará en la lista de usuarios. No obstante, la cuenta sigue almacenada en el instrumento. Para ver o volver a activar esta cuenta, marque **<Show Inactive>** (ver la Pantalla 10.16) y seguir el mismo procedimiento en la sección 10.2.7 ´Cambiar las funciones asignadas a un usuario o grupo LDAP´.

10.2.9 Eliminación de usuarios LDAP

1. Seleccionar un usuario LDAP o un grupo LDAP de la lista de usuarios.
2. En la página de configuración de usuarios, tocar **<Delete>** (ver la Pantalla 10.17).



Pantalla 10.17: Eliminación de un usuario LDAP

3. Tocar <Save> en la parte inferior para volver a la lista de usuarios.

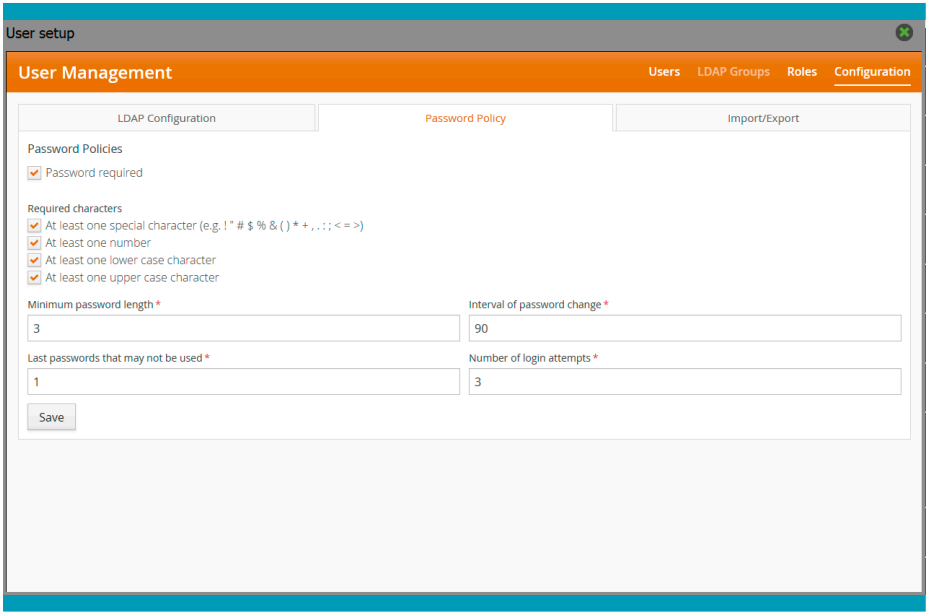
10.3 Configuración de la política de contraseñas

Para configurar la política de contraseñas, tocar <Configuration> en la esquina superior derecha y seleccionar la pestaña <Password Policy>. Podrá configurar lo siguiente:

- Caracteres necesarios
- Longitud de la contraseña
- Tiempo hasta la caducidad de la contraseña (en días)
- Últimas contraseñas que no se pueden utilizar
- Número máximo de intentos de inicio de sesión

Nota: El cambio de la política de contraseñas solo afectará a los usuarios creados posteriormente. Los usuarios ya creados no se verán afectados.

Nota: La política de contraseñas es anulada por la política de contraseñas LDAP para la cuenta LDAP.



Pantalla 10.18: Configuración de la política de contraseñas

10.4 Importar y exportar ajustes de administración de usuarios

La configuración del UMS se puede transferir de un instrumento a otro. El proceso consta de dos fases:

(1) Copia entre la memoria USB flash y la carpeta de intercambio UMS mediante UMS Exchange Tool

(2) Importación/exportación al UMS en la configuración de la administración de usuarios.

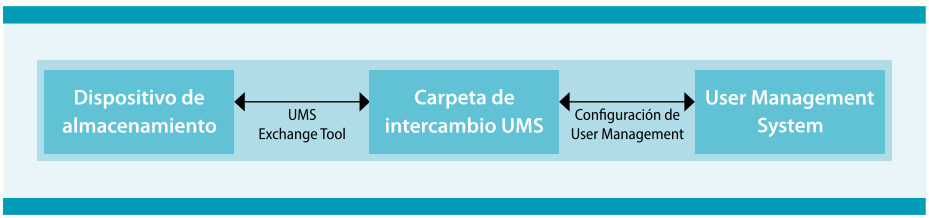


Figura 10.2: User Management System (Sistema de administración de usuarios)

El procedimiento de ejemplo se aplica a los dos archivos siguientes:

- Importe archivos de certificado SSL (Secure Sockets Layer) para configurar una conexión LDAP segura.

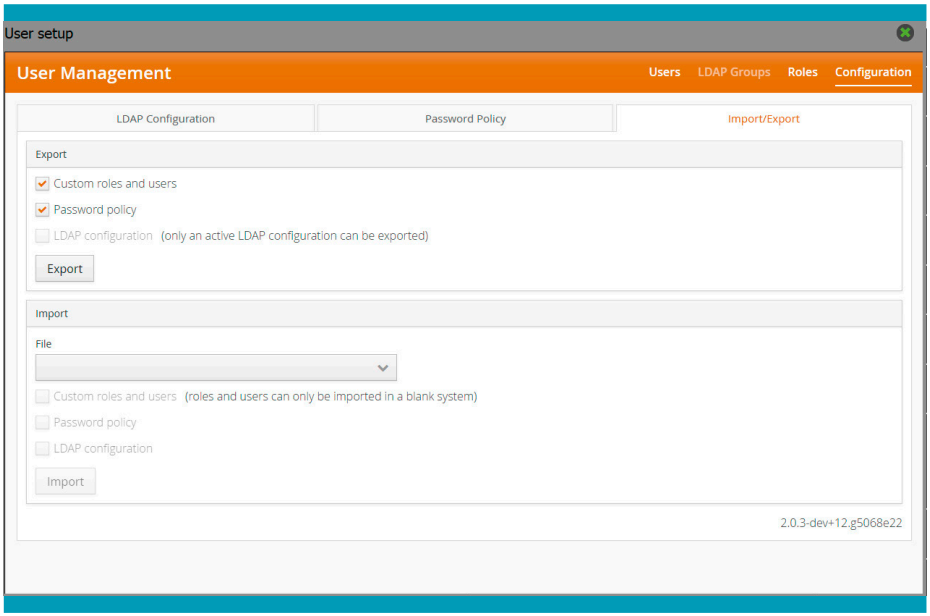
- Importe y exporte archivos de configuración del UMS para realizar copias de seguridad o reutilizarlos en otras instancias del UMS.

Nota: Solo los usuarios del UMS con la función de administrador «Administration tools user» podrán acceder a esta aplicación.

10.4.1 Exportar ajustes de administración de usuarios

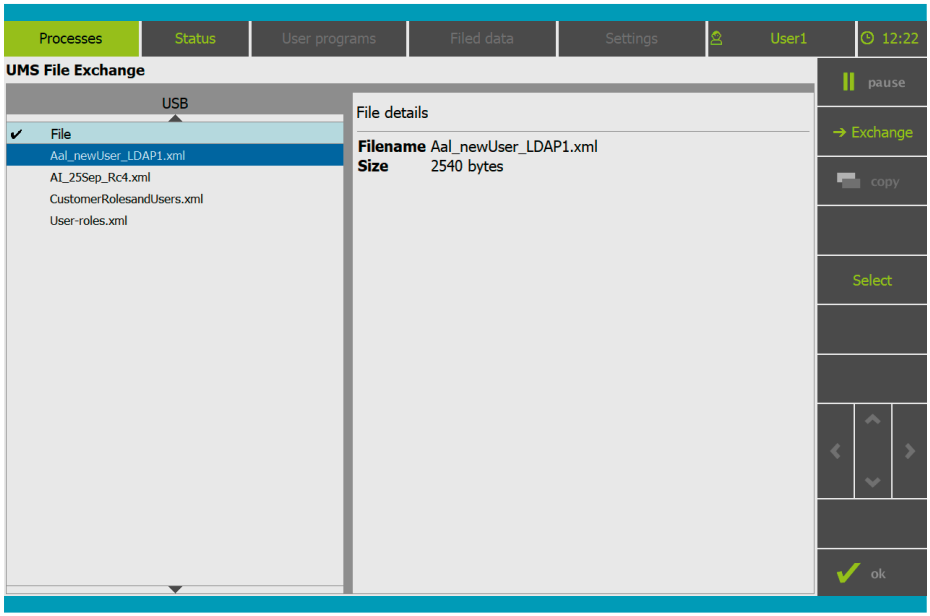
IMPORTANTE
Los roles y los usuarios solo se pueden importar en un sistema vacío.

1. Insertar una memoria USB flash.
2. Ir a <User Management> ▸ <Configuration> ▸ <Import/Export>. Tocar <Export>. Los ajustes del UMS se exportarán a la carpeta de intercambio UMS del instrumento.



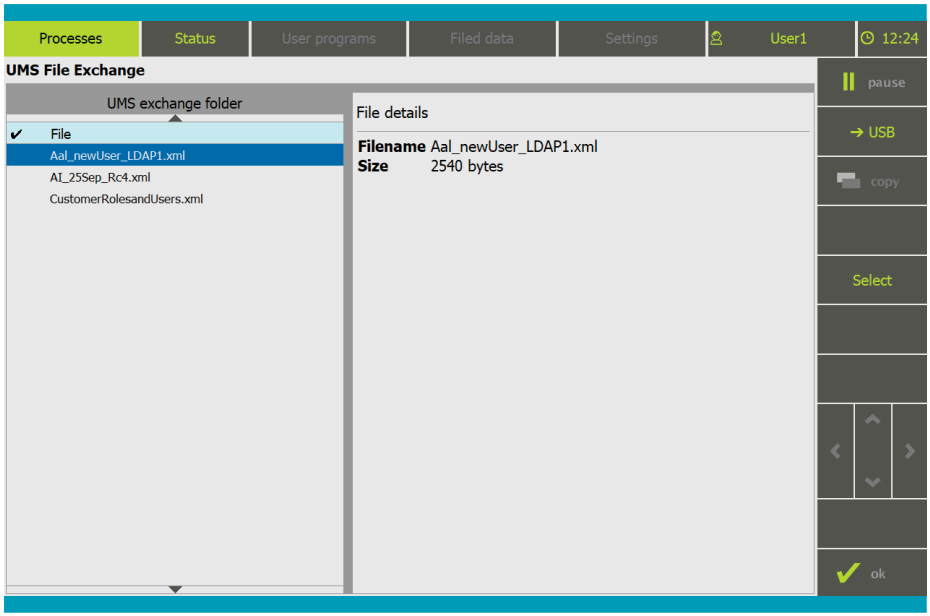
Pantalla 10.19: Submenú «Configuration» (Configuración) con «Import/Export» (Importar/Exportar) activo

3. Para acceder a <UMS File Exchange>, ir a <Settings> ▸ <Tools>, <UMS File Exchange> y tocar <run>.
4. Si aparece USB en la columna izquierda, tocar <Exchange> para enumerar el contenido de la carpeta de intercambio UMS (ver la Pantalla 10.20). Los archivos de la carpeta de intercambio del UMS se mostrarán en la columna izquierda (ver la Pantalla 10.21).



Pantalla 10.20: Archivo seleccionado y botón de menú «Exchange»

5. Seleccionar los archivos que desee transferir al UMS y tocar <Select>.
6. Una vez seleccionados todos los archivos a transferir, tocar <Copy> para iniciar la transferencia.



Pantalla 10.21: Carpeta de intercambio UMS con archivos seleccionados

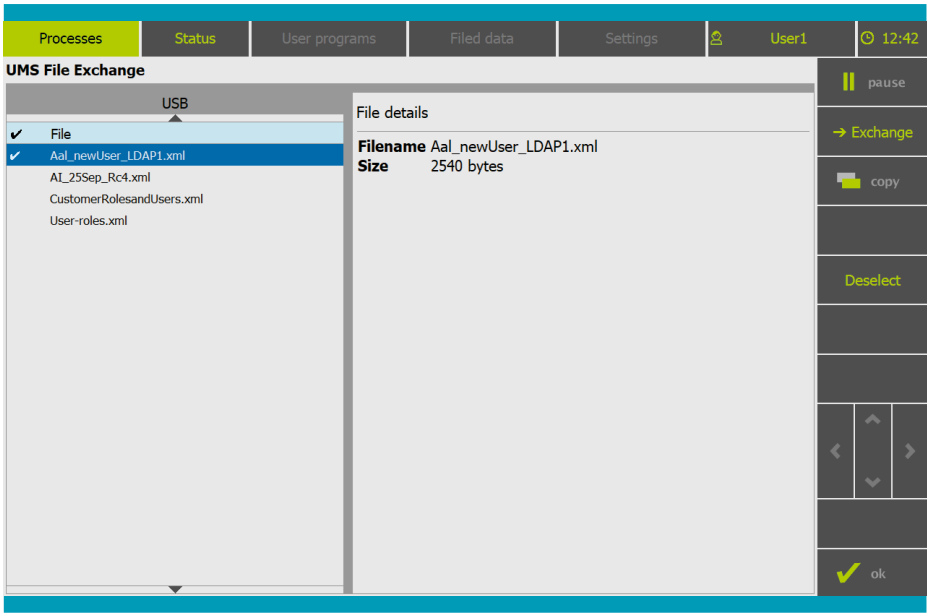
10.4.2 Importar ajustes del UMS

1. Insertar una memoria USB flash.
   Asegurarse de que los archivos se encuentren en la carpeta raíz de la unidad USB flash (no se reconocerán los archivos de las subcarpetas).

2. Ir a <Process> ▸ <Tools>, <UMS File Exchange> y tocar <run> para acceder a la herramienta <UMS File Exchange>. Se mostrará una lista de archivos en el lado izquierdo.

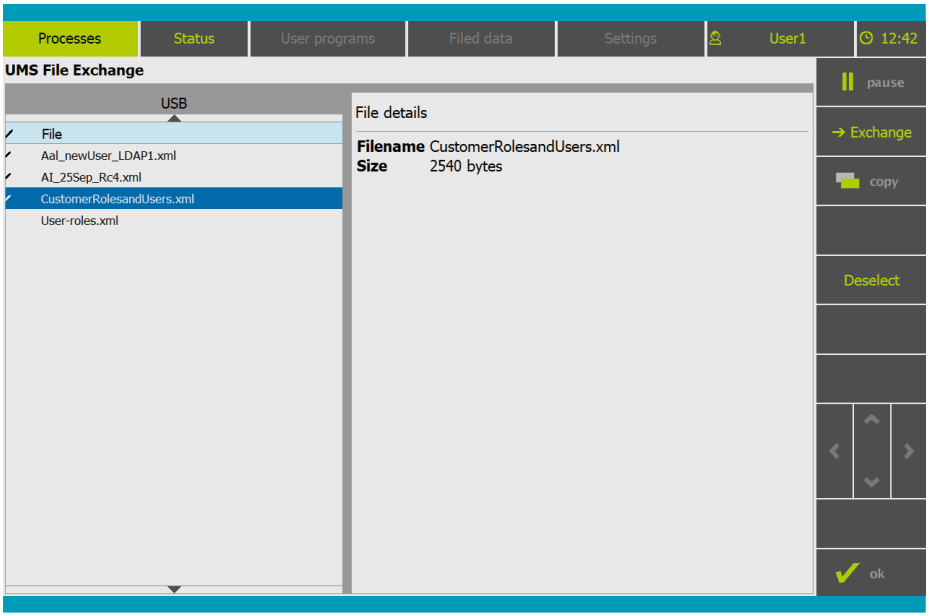
3. Cuando se muestre la carpeta de intercambio UMS, tocar <USB> en la barra de herramientas. Asegurarse de que se indique <USB> en la parte superior de la lista de archivos en la columna izquierda.

4. Seleccionar los archivos que desee transferir y tocar <Select>. Para anular la selección del archivo, elegir un archivo seleccionado y tocar <Deselect>.



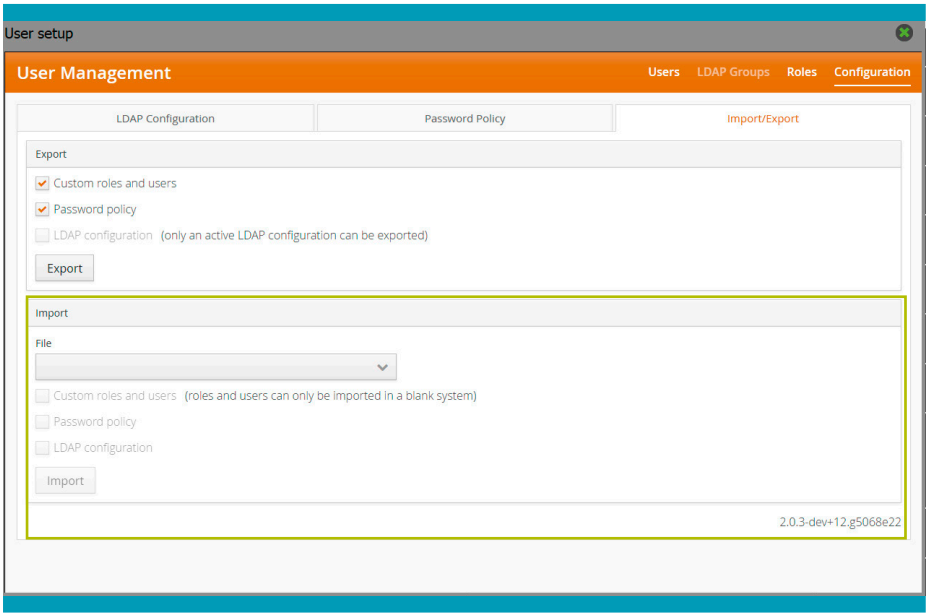
Pantalla 10.22: Archivo seleccionado y botón de menú «Select»

5. Una vez seleccionados todos los archivos que desee transferir, tocar <Copy> para iniciar la transferencia.



Pantalla 10.23: Carpeta USB con archivos seleccionados

6. Ir a <User setup> ▸ <Configuration> ▸ <Import/Export>. Seleccionar el archivo en <Import> y tocar <Import>.



Pantalla 10.24: Submenú «Configuration» con pestaña «Import/Export»

11 Resolución de problemas

En cualquier otro caso de fallo de funcionamiento del instrumento o de fallo del proceso, póngase en contacto con Miltenyi Biotec Technical Support:

+49 2204 8306-3803
technicalsupport@miltenyi.com

Visite www.miltenyibiotec.com para obtener información de contacto de su Miltenyi Biotec Technical Support local.

12
Aviso legal

12.1 Garantía limitada

Salvo que se indique en una declaración de garantía específica, que puede acompañar a este producto de Miltenyi Biotec, o a menos que se acuerde lo contrario por escrito por un representante debidamente autorizado de Miltenyi Biotec, la garantía de Miltenyi Biotec para los productos comprados directamente a Miltenyi Biotec estará sujeta a los términos y condiciones de venta bajo los cuales le fue proporcionada por la respectiva organización de ventas de Miltenyi Biotec. Estas condiciones están disponibles a petición o en www.miltenyibiotec.com. Los términos y condiciones de venta aplicables pueden variar según el país y la región. Nada de lo aquí expuesto debe interpretarse como una garantía adicional.

En el caso de los productos comprados a terceros minoristas o revendedores (por ejemplo, comprados a un proveedor de servicios local autorizado de Miltenyi Biotec), pueden aplicarse términos y condiciones diferentes.

Para determinar la garantía que acompaña a su producto, consultar el albarán, la factura, el recibo u otra documentación de venta. Algunos componentes de una combinación de productos que haya adquirido pueden tener una garantía más corta que la que figura en el albarán, la factura, el recibo u otra documentación de venta (por ejemplo, productos sujetos a caducidad y obsolescencia).

La garantía de Miltenyi Biotec para este producto solo cubre los problemas del producto causados por defectos en el material o la mano de obra durante el uso normal. No cubre los problemas del producto causados por cualquier otra razón, incluidos, entre otros, los problemas del producto debidos a su uso de una manera distinta a la descrita específicamente en este manual, por ejemplo: uso inapropiado o inadecuado; montaje o instalación incorrecta por parte de un operario o un tercero; desgaste razonable; operación, manipulación, almacenamiento, servicio o mantenimiento negligentes o incorrectos; incumplimiento de las instrucciones de funcionamiento; modificación no autorizada de o a cualquier parte de este producto; o uso de consumibles, accesorios o materiales de trabajo inapropiados.

La garantía de Miltenyi Biotec no cubre los productos vendidos TAL CUAL o CON TODOS LOS FALLOS ni los consumibles. Nada de lo aquí expuesto debe interpretarse como una garantía adicional.

Se debe informar inmediatamente a Miltenyi Biotec si se hace una reclamación bajo dicha garantía. Si se produce un defecto de material o de fabricación dentro del periodo de garantía, Miltenyi Biotec tomará las medidas oportunas para restablecer la plena capacidad de uso del instrumento.

Limitación en caso de daños
Miltenyi Biotec no se responsabilizará de ningún daño accidental o consecuente por incumplimiento de cualquier garantía o condición expresa o implícita relacionada con este producto.

Algunos países, estados o jurisdicciones no permiten la exclusión ni limitación de los daños accidentales o consecuentes, por lo que las limitaciones o exclusiones anteriores pueden no ser aplicables en su caso. Esta declaración de garantía le otorga derechos legales específicos y puede tener otros derechos, que varían de un estado a otro o de una jurisdicción a otra.

12.2 Marcas comerciales

CliniMACS, CentriCult y el logotipo de Miltenyi Biotec son marcas comerciales registradas o marcas comerciales de Miltenyi Biotec B.V. & Co. KG y/o de sus filiales en distintos países del mundo.

APÉNDICE

Cada proceso, herramienta y ajuste se asocia a derechos específicos, p. ej., el derecho a «Mostrar» y el derecho a «Iniciar». Con el derecho de «Mostrar», la herramienta/el proceso/el ajuste aparecerá en la pestaña de Proceso/Ajustes. Para poder ejecutar el proceso/la herramienta/el ajuste, es necesario asignar el derecho de «Inicio» a la función. Los componentes más complicados, como el audit trail y la administración de usuarios, tienen derechos más detallados.

Proceso/Herramienta/Ajustes/ Componente	Detalles
Process xxx right (Derecho para el proceso xxx)	• Show process xxx (Mostrar el proceso xxx) • Start process xxx (Iniciar el proceso xxx)
Tool xxx right (Derecho para la herramienta xxx) • Backup Filed Data (Copia de seguridad de los archivos) • Custom Files (Archivos personalizados) • Instrument check (Chequeo del instrumento) • License (Licencia) • N2 Settings (Ajustes N2) • Ajustes de red • Set Time (Ajustar la hora) • Settings Exchange (Ajustes del intercambio) • SetVolume (Ajustar el volumen) • Apagado • UMSFileExchange exchange (intercambio de archivos para el sistema de gestión de usuarios) • UMSSettings settings Process xxx right (Ajustes en el sistema de gestión de usuarios en cuanto al derecho para el proceso xxx)	• Show tool xxx (Mostrar la herramienta xxx) • Start tool xxx (Iniciar la herramienta xxx)
Derecho para Setting xxx (Ajuste xxx)	• Show setting xxx (Mostrar ajuste xxx)

Proceso/Herramienta/Ajustes/ Componente	Detalles
• Info (Información) • System settings (Ajustes sistema)	• Start setting xxx (Iniciar ajuste xxx)
Instrument (Instrumento)	• Log file access via FTP (Acceso al archivo de registro a través de FTP) • Show injected programs (Mostrar programas inyectados) • Start injected programs (Iniciar programas inyectados)
User Management (Administración de usuarios)	• Assign role (Asignar función) • Configure LDAP connection (Configurar conexión LAPD) • Create role (Crear función) • Create user (Crear usuario) • Export (Exportar) • Import (Importar) • Read Password Policy (Leer política de contraseñas) • Read details of foreign account (Leer datos de cuenta exterior) • Read details of own account (Leer datos de la cuenta propia) • Read own user details (Leer datos de usuario propios) • Read rights of foreign account (Derechos de lectura de una cuenta exterior) • Read rights of own account (Derechos de lectura de la cuenta propia) • Read role (Leer función) • Read user details (Leer datos usuario) • Set user active (Ajustar usuario a activo) • Set user inactive (Ajustar usuario a inactivo) • Unlock user (Desbloquear usuario) • Update Password Policy (Actualizar política de contraseñas) • Update own user details (Actualizar datos de usuario propios) • Update role (Actualizar función) • Update user details (Actualizar datos de usuario)
audit trail Management (Administración audit trail)	• Export audit trail events (Exportar eventos de audit trail) • Read audit trail events (Leer eventos de audit trail) • Reset audit trail events (Restablecer eventos de audit trail)

Tabla A.1: Resumen de los derechos definidos en el software

Funciones predeterminadas

Funciones	Herramientas/derechos
ATS User (Usuario ATS)	Usuario del componente audit trail • audit trail Management (Administración audit trail)
Administration tools user (Usuario de herramientas de administración)	• Customer settings (Ajustes del cliente) • Network settings (Ajustes de red) • Platform configuration settings (Ajustes de configuración de la plataforma) • Settings exchange (Ajustes del intercambio) • System settings (Ajustes sistema) • UMSFileExchange exchange (intercambio de archivos para el sistema de gestión de usuarios)
File management user (Usuario de administración de archivos)	Un usuario que utiliza herramientas para administrar archivos • Backup Filed Data (Copia de seguridad de los archivos) • Custom Files (Archivos personalizados) • Log file access via FTP (Acceso al archivo de registro a través de FTP)
File system access (Acceso al sistema de archivos)	Acceso a ejecutables arbitrarios en el sistema de archivos – sin acceso a derechos
Support tools user (Usuario de herramientas de apoyo)	Un usuario que puede utilizar herramientas que apoyan la ejecución de aplicaciones • Chamber In (Introducir cámara) • Chamber out (Extraer cámara) • FormU Sensor (Sensor FormU) • FormU Valves (Válvulas FormU) • FRAMrd • Gasmix Settings (Ajustes de mezcla de gases) • Instrument Check (Chequeo del instrumento) • Module Settings (Ajustes del módulo) • Sealer (Sellador)
UM Administrator	Administrador del componente de administración de usuarios User Management – todos los derechos
UM Service (Servicio UM)	Service User (Usuario de servicio) • User Management – all rights (User Management – todos los derechos)
UM User	Customer User (Cliente usuario) • User Management: Read details for own account (Leer detalles de la cuenta propia) • User Management: Read rights for own account (Leer derechos de la cuenta propia)

Tabla A.2: Funciones predeterminadas

NOTAS



Miltenyi Biotec

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

Estados Unidos/Canadá
Miltenyi Biotec, Inc.
1201 Clopper Road
Gaithersburg, MD 20878
Estados Unidos
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
Países Bajos
macsnl@miltenyi.com
Servicio de atención para:
Países Bajos
0800 4020120
0800 4020100
Bélgica
0800 94016
0800 99626
Luxemburgo
800 24971
800 24984

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

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

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

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

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

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

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

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

Países Nórdicos y Bálticos
Miltenyi Biotec Norden AB
Medicon Village
Scheeletorget 1
223 81 Lund
Suecia
macsse@miltenyi.com
Servicio de atención para:
Suecia
0200 111 800
+46 280 72 99
Dinamarca
80 20 30 10
+46 46 280 72 99
Noruega, Finlandia, Islandia y países bálticos
+46 46 280 72 80
+46 46 280 72 99

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

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

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

www.miltenyibiotec.com

Miltenyi Biotec proporciona productos y servicios en todo el mundo. Visite **www.miltenyibiotec.com/local** para localizar su persona de contacto de Miltenyi Biotec más cercana.

CliniMACS, CentriCult y el logotipo de Miltenyi Biotec son marcas comerciales registradas o marcas comerciales de Miltenyi Biotec B.V. & Co. KG y/o de sus filiales en distintos países del mundo. Copyright © 2026 Miltenyi Biotec y/o sus filiales. Todos los derechos reservados.

210-005-264/01 | Edición: 2026-03