SCIEX
The Power of Precision

Software SCIEX OS

Guía del director de laboratorio

RUO-IDV-05-7370-ES-I

Junio de 2022

Este documento se proporciona a los clientes que han adquirido un equipo SCIEX, para que lo usen durante el funcionamiento de dicho equipo SCIEX. Este documento está protegido por derechos de propiedad y queda estrictamente prohibida cualquier reproducción total o parcial, a menos que SCIEX lo autorice por escrito.

El software que se describe en este documento se proporciona bajo un acuerdo de licencia. Está legalmente prohibida la copia, modificación o distribución del software en cualquier medio, a menos que se permita específicamente en el acuerdo de licencia. Además, es posible que el acuerdo de licencia prohíba igualmente desensamblar, realizar operaciones de ingeniería inversa o descompilar el software con cualquier fin. Las garantías son las indicadas en ese documento.

Algunas partes de este documento pueden hacer referencia a otros fabricantes o sus productos, que pueden contener piezas cuyos nombres se han registrado como marcas comerciales o funcionan como marcas comerciales de sus respectivos propietarios. El uso de dichos nombres en este documento pretende únicamente designar los productos de esos fabricantes suministrados por SCIEX para la incorporación en su equipo y no supone ningún derecho o licencia de uso, ni permite a terceros el empleo de dichos nombres de productos o fabricantes como marcas comerciales.

Las garantías de SCIEX están limitadas a aquellas garantías expresas proporcionadas en el momento de la venta o licencia de sus productos, y son representaciones, garantías y obligaciones únicas y exclusivas de SCIEX. SCIEX no ofrece otras garantías de ningún tipo, expresas o implícitas, incluyendo, entre otras, garantías de comercialización o adecuación para un fin específico, ya se deriven de un estatuto, cualquier tipo de legislación, uso comercial o transcurso de negociación; SCIEX rechaza expresamente todas estas garantías y no asume ninguna responsabilidad, general o accidental, por daños indirectos o derivados del uso por parte del comprador o por cualquier circunstancia adversa derivada de este.

Para uso exclusivo en investigación. No para uso en procedimientos diagnósticos.

AB Sciex Pte. Ltd.
Blk33, #04-06 Marsiling Industrial Estate Road 3
Woodlands Central Industrial Estate, Singapore 739256

Tabla de contenido

Introducción 1

La información contenida en este manual está destinada a dos tipos principales de usuarios:

- El administrador del laboratorio, que es el responsable del funcionamiento y uso diario del software SCIEX OS y la instrumentación conectada desde un punto de vista funcional.
- El administrador del sistema, que se encarga de la seguridad del sistema y la integridad y los datos del sistema.

Descripción general de la configuración de seguridad 2

En esta sección se describe la forma en que los componentes de control de acceso y auditoría del software SCIEX OS trabajan en colaboración con los componentes de control de acceso y auditoría de Windows. Además se describe cómo configurar la seguridad de Windows antes de instalar SCIEX OS.

Seguridad y cumplimiento normativo

SCIEX OS proporciona:

- Capacidades de administración personalizables para cumplir los requisitos normativos y de investigación
- Herramientas de seguridad y auditoría para el cumplimiento de 21 CFR Part 11 sobre el uso de mantenimiento de registros electrónicos.
- Gestión eficiente y flexible del acceso a las funciones principales del espectrómetro de masas
- Acceso controlado y auditado a datos e informes esenciales
- Gestión sencilla de la seguridad vinculada al sistema de seguridad de Windows

Requisitos de seguridad

Los requisitos de seguridad varían en función de su aplicación, es decir, si se trata de entornos relativamente abiertos, como laboratorios de investigación o académicos, o de entornos estrictamente regulados, como los laboratorios de investigación.

SCIEX OS y sistema de seguridad de Windows: funcionamiento conjunto

SCIEX OS y el NTFS (sistema de archivos de nueva tecnología) de Windows disponen de funciones de seguridad diseñadas para controlar el acceso al sistema y a los datos.

El sistema de seguridad de Windows proporciona un nivel de protección superior, ya que obliga a los usuarios a iniciar sesión en la red mediante una identificación de usuario y una contraseña únicas. Como resultado, solo los usuarios reconocidos por la configuración de seguridad de Windows local o de la red tienen acceso al sistema. Para obtener más información, consulte la sección Configuración del sistema de seguridad de Windows.

SCIEX OS tiene los siguientes modos de acceso seguro al sistema:

- Modo mixto
- Modo integrado (predeterminado)

Para obtener más información sobre los modos y la configuración de seguridad, consulte la sección Configuración del modo de seguridad.

SCIEX OS también proporciona funciones completamente configurables que son independientes de los grupos de usuarios asociados a Windows. Mediante el uso de funciones, el director de laboratorio puede controlar el acceso al software y al espectrómetro de masas a través de las funcionalidades disponibles para cada función. Para obtener más información, consulte la sección Configuración del acceso al software SCIEX OS.

Pistas de auditoría en SCIEX OS y Windows

Las funciones de auditoría de SCIEX OS, junto con los componentes de auditoría integrados de Windows, son fundamentales para la creación y gestión de registros electrónicos.

SCIEX OS proporciona un sistema de pistas de auditoría para cumplir los requisitos del mantenimiento de registros electrónicos. Estas pistas de auditoría independientes registran:

- Cambios en la tabla de calibración de masas o en la tabla de resoluciones, cambios en la configuración del sistema y eventos de seguridad.
- La creación y modificación de eventos para proyectos, ajuste, lotes, datos, métodos de procesamiento, archivos de plantilla de informe, así como eventos de apertura, cierre de módulos y de impresión. Los eventos de eliminación registrados en la pista de auditoría incluyen la eliminación de funciones y la eliminación de usuarios en SCIEX OS.
- La creación y modificación de la información de muestras, los parámetros de integración de picos y el método de procesamiento integrado en una tabla de resultados.

Nota: SCIEX OS no audita la creación ni los cambios en métodos de MS, métodos de LC, lotes o métodos de procesamiento. Estos archivos sirven como plantillas. Los valores de los parámetros se leen en el momento de la adquisición o el procesamiento y se aplican a la tarea. Para los métodos de MS, los métodos de LC y los lotes, los valores de los parámetros se registran en los archivos wiff y wiff2. Para los métodos de procesamiento, se registran en el archivo qsession. Estos archivos sirven como registros electrónicos para esta información.

Para ver una lista completa de los eventos de auditoría, consulte la sección Eventos de auditoría.

SCIEX OS utiliza el registro de eventos de la aplicación para recopilar información sobre el funcionamiento del software. Utilice este registro como ayuda para solucionar problemas. Contiene información detallada de las interacciones entre el espectrómetro de masas, el dispositivo y el software.

Windows conserva registros de eventos que recopilan una amplia variedad de eventos relacionados con la seguridad, el sistema y la aplicación. En la mayoría de los casos, la función de auditoría de Windows está diseñada para registrar eventos inusuales, como los fallos de inicio de sesión. El administrador puede configurar este sistema para registrar diferentes tipos de eventos, entre ellos, el acceso a archivos específicos o actividades administrativas de Windows. Para obtener más información, consulte la sección Auditorías del sistema.

Pautas para la seguridad de los usuarios: copias de seguridad

La realización de la copia de seguridad de los datos de cliente es responsabilidad del cliente. Aunque el personal de servicio y soporte técnico de SCIEX puede ofrecer asesoramiento y recomendaciones sobre la copia de seguridad de los datos de cliente, es responsabilidad del cliente asegurarse de que se realiza la copia de seguridad de los datos conforme a las políticas, las necesidades y los requisitos legales del cliente. La frecuencia y la cobertura de la copia de seguridad de los datos de cliente deberían ser proporcionales a los requisitos organizativos y a la criticidad de los datos que se generan.

Los clientes deben asegurarse de que las copias de seguridad son funcionales, ya que constituyen un componente vital de la gestión de datos en general y resultan esenciales para llevar a cabo una recuperación en caso de que se produzca un ataque malintencionado o un fallo de hardware o software. No haga una copia de seguridad del ordenador durante la adquisición de datos o asegúrese de que el software de copia de seguridad omite los archivos que se estén adquiriendo. Recomendamos encarecidamente que se realice una copia de seguridad completa del ordenador antes de llevar a cabo una actualización de seguridad o cualquier reparación del ordenador. Esto facilitará restaurar los datos en el improbable caso de que un parche de seguridad afecte a la funcionalidad de alguna aplicación.

21 CFR Parte 11

SCIEX OS contiene los controles técnicos para cumplir la norma 21 CFR Parte 11 con la implementación de:

- Modos de seguridad mixto e integrado asociados al sistema de seguridad de Windows.
- Acceso controlado a las funcionalidades mediante la asignación de funciones personalizables.
- Pistas de auditoría para el funcionamiento del instrumento, la adquisición y revisión de datos y la generación de informes.
- Firmas electrónicas con una combinación de ID de usuario y contraseña.
- Configuración adecuada del sistema operativo Windows.
- Procedimientos y formación apropiada en la empresa.

SCIEX OS está diseñado para utilizarlo como parte de un sistema conforme a la norma 21 CFR Parte 11 y se puede configurar para adecuarse al cumplimiento de dicha norma. Que el uso del software SCIEX OS cumpla la norma 21 CFR Parte 11 depende del uso y configuración real de SCIEX OS en el laboratorio.

Los servicios profesionales de SCIEX ofrecen servicios de validación. Para obtener más información, póngase en contacto con complianceservices@sciex.com.

Nota: No deje el software Instrument Parameters Converter en un sistema validado. Está diseñado para la transferencia inicial de la configuración del instrumento del software Analyst a SCIEX OS. Asegúrese de eliminar el software Instrument Parameters Converter del ordenador después de utilizarlo.

Configuración del sistema

La configuración del sistema suelen llevarla a cabo administradores de red o usuarios con derechos de administración local y de red.

Configuración del sistema de seguridad de Windows

El sistema implementa las siguientes restricciones para las cuentas de usuario locales de Windows:

- La contraseña de Windows se debe cambiar cada 90 días.
- La contraseña de Windows no se puede reutilizar al menos durante la siguiente iteración. Es decir, no puede ser igual que la contraseña anterior.
- La contraseña de Windows debe tener un mínimo de ocho caracteres.
- La contraseña de Windows debe cumplir al menos dos de los cuatro requisitos siguientes para que sea lo suficientemente compleja:
  - Una letra mayúscula
  - Una letra minúscula
  - Un valor numérico
  - Un carácter especial (como ! @ # $ % ^ &)
- El nombre de usuario de Windows no debe ser **admin**, **administrator** ni **demo**.

El administrador de SCIEX OS debe disponer del privilegio para cambiar los permisos de la carpeta SCIEX OS Data. Si esta carpeta está en un ordenador local, recomendamos que el administrador del software sea parte del grupo de administradores locales.

Para asegurarse de que todos los usuarios cuentan con el acceso necesario a los recursos para la adquisición en red, el administrador de la red puede definir una cuenta de red segura (SNA) en el recurso de red. Esta cuenta debe tener permisos de escritura para la carpeta de red que contiene el directorio principal. Se define como la SNA en las propiedades del directorio principal.

Usuarios y grupos

SCIEX OS utiliza los nombres de usuario y las contraseñas registradas en la base de datos de seguridad del controlador de dominio principal o en Active Directory. Las contraseñas se gestionan mediante las herramientas proporcionadas con Windows. Para obtener más información sobre añadir y configurar personas y funciones, consulte la sección Configuración del acceso al software SCIEX OS.

Compatibilidad con Active Directory

Cuando se añaden usuarios en el espacio de trabajo Configuración SCIEX OS, hay que especificar cuentas de usuario en formato nombre principal de usuario (UPN). Se admiten las siguientes versiones de Active Directory:

- Servidores Windows 2012.

- Clientes Windows 7 de 64 bits
- Clientes Windows 10 de 64 bits

Sistema de archivos de Windows

En SCIEX OS, los archivos y directorios deben guardarse en una partición del disco duro que utilice el formato NTFS, que puede controlar y auditar el acceso a los archivos SCIEX OS. El sistema de tabla de asignación de archivos (FAT) no puede controlar ni auditar el acceso a las carpetas o los archivos y, por lo tanto, no es adecuado para proporcionar un entorno seguro.

Permisos de archivos y carpetas

Para gestionar la seguridad, el administrador de SCIEX OS debe disponer del privilegio para cambiar los permisos de la carpeta `SCIEX OS Data`. El acceso debe configurarlo el administrador de red.

Nota: Tenga en cuenta el nivel de acceso que necesitan los usuarios para la unidad, el directorio raíz y las carpetas de proyecto en cada ordenador. Configure las opciones de uso compartido y los permisos asociados. Para obtener más información sobre el uso compartido de archivos, consulte la documentación de Windows.

Para obtener información sobre los permisos para los archivos y carpetas de SCIEX OS, consulte la sección Control de acceso.

Auditorías del sistema

Se puede habilitar la función de auditoría del sistema Windows para detectar brechas de seguridad o intrusiones en el sistema. Las auditorías se pueden establecer para que registren diferentes tipos de eventos relacionados con el sistema. Por ejemplo, se puede habilitar la función de auditoría para registrar en el registro de eventos cualquier intento de inicio de sesión correcto o incorrecto para acceder al sistema.

Registros de eventos

El Visor de eventos de Windows registra los eventos auditados en el registro de seguridad, el registro del sistema y el registro de la aplicación.

Personalice los registros de eventos de la forma siguiente:

- Configurar un tamaño adecuado de registro de eventos.
- Habilitar la sobrescritura automática de eventos antiguos.
- Ajustar la configuración de seguridad del equipo de Windows.

Es posible implementar un proceso de revisión y almacenamiento. Para obtener más información sobre la configuración de seguridad y las directivas de auditoría, consulte la documentación de Windows.

Alertas de Windows

Configure la red para que se envíe un mensaje automático a una persona específica, como el administrador del sistema, en caso de que se produzca un problema relacionado con el sistema o el usuario en el mismo ordenador o en ordenadores distintos.

- Tanto en el ordenador emisor como en el receptor, inicie el servicio Messenger en el panel de control de Servicios de Windows.
- En el ordenador emisor, inicie el servicio Alert en el panel de control de Servicios de Windows.

Para obtener más información acerca de cómo crear un objeto de alerta, consulte la documentación de Windows.

Licencias electrónicas 3

Para SCIEX OS, las licencias electrónicas puede estar limitadas a nodos o basadas en servidor. Para el software Central Administrator Console (CAC), las licencias electrónicas solo pueden estar limitadas a nodos.

Puede que más adelante se necesite el ID de activación para algún servicio o llamada de asistencia técnica. Para acceder al ID de activación de la licencia limitada a nodos o basada en servidor:

- En el espacio de trabajo Configuración, haga clic en **Licenses**, en la ventana de SCIEX OS.

Nota: Asegúrese de renovar la licencia antes de que venza.

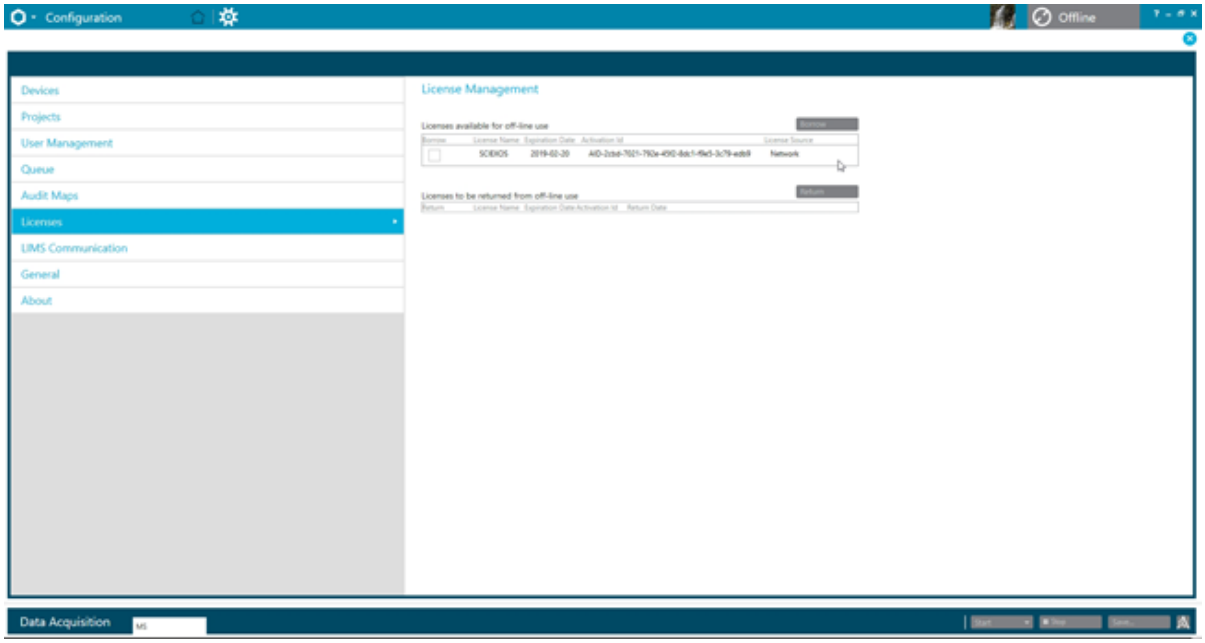
Préstamo de una licencia electrónica basada en servidor

Se necesita una licencia para usar SCIEX OS. Si se usa una licencia basada en servidor, los usuarios que quieran trabajar fuera de línea pueden reservar una licencia para un máximo de 7 días. Durante este periodo, la licencia electrónica prestada es exclusiva para el ordenador.

Nota: Este procedimiento no es aplicable en el caso del software Central Administrator Console (CAC).

1. Abra el espacio de trabajo Configuration.
2. Haga clic en **Licenses**.
   La tabla Licenses available for off-line use muestra todas las licencias disponibles para préstamo.

Figura 3-1: Gestión de licencias: préstamo de una licencia



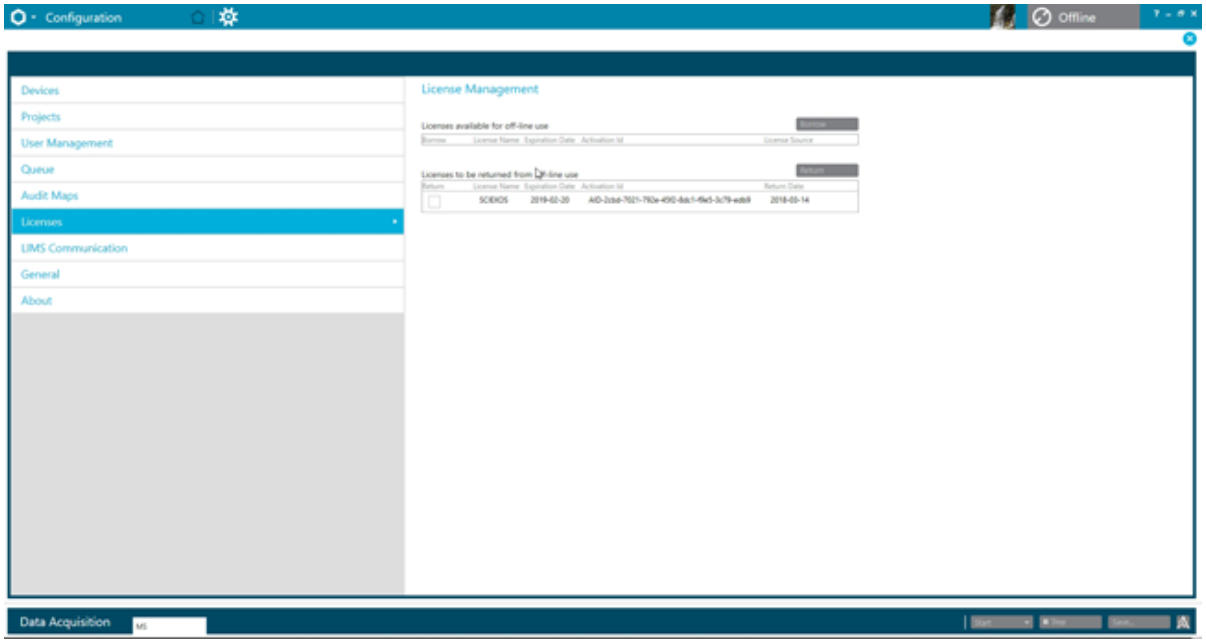
3. Seleccione la licencia que desee pedir prestada y haga clic en **Borrow**.

Devolución de una licencia electrónica basada en servidor

Nota: Este procedimiento no es aplicable en el caso del software Central Administrator Console (CAC).

1. Abra el espacio de trabajo Configuration.
2. Haga clic en **Licenses**.
   La tabla Licenses to be returned from off-line use muestra todas las licencias que se pueden devolver, es decir, todas las licencias que ha tomado prestadas este ordenador.

Figura 3-2: Gestión de licencias: devolución de una licencia



3. Seleccione la licencia que desee devolver y haga clic en **Return**.

Control de acceso 4

En esta sección se describe cómo controlar el acceso a AnalystSCIEX OS. Para controlar el acceso a SCIEX OS, el administrador realiza las siguientes tareas:

Nota: Para realizar las tareas en esta sección, el usuario debe tener privilegios de administrador local para la estación de trabajo en la que se esté instalando el software.

- Instalar y configurar SCIEX OS.
- Añadir y configurar usuarios y funciones.
- Configurar el acceso a los proyectos y a los archivos de proyecto en el directorio principal.

Este procedimiento proporciona instrucciones para la administración local de SCIEX OS. Para la administración centralizada de SCIEX OS, consulte la sección: Central Administrator Console

Nota: Los cambios realizados en la configuración de SCIEX OS tendrán efecto después de reiniciar SCIEX OS.

Ubicación de la información de seguridad

Toda la información de seguridad se guarda en el ordenador local, en la carpeta `C:\ProgramData\SCIEX\Clearcore2.Acquisition`, en un archivo denominado `Security.data`.

Operaciones de seguridad del software

SCIEX OS funciona con los componentes de seguridad, aplicación y auditoría de eventos del sistema de las herramientas administrativas de Windows.

Configure la seguridad en los siguientes niveles:

- Autenticación de Windows: acceso al ordenador.
- Autorización de Windows: acceso a archivos y carpetas.
- Autenticación de SCIEX OS: capacidad de abrir SCIEX OS.
- Autorización de SCIEX OS: acceso a la funcionalidad en SCIEX OS.

Para ver la lista de tareas para configurar la seguridad, consulte la Tabla 4-1. Para ver las opciones para configurar los distintos niveles de seguridad, consulte la Tabla 4-2.

Tabla 4-1: Flujo de trabajo para la configuración de seguridad

Tarea	Procedimiento
Instalar SCIEX OS.	Consulte el documento *Guía de instalación del software SCIEX OS*.
Configurar el acceso a SCIEX OS.	Consulte la sección Configuración del acceso al software SCIEX OS.
Configurar el sistema de seguridad de archivos y el sistema NTFS de Windows.	Consulte la sección Configuración del acceso a proyectos y archivos de proyectos.

Tabla 4-2: Opciones de configuración de seguridad

Opción	CFR 21 Parte 11
Seguridad de Windows	
Configurar usuarios y grupos (autenticación).	Sí
Habilitar auditoría de Windows y auditoría de archivos y directorios.	Sí
Establecer permisos de archivo (autorización).	Sí
Instalación de SCIEX OS	
Instalar SCIEX OS.	Sí
Abrir el visor de eventos para inspeccionar la instalación.	Sí
Seguridad del software	
Seleccionar el modo de seguridad.	Sí
Configurar los usuarios y funciones de SCIEX OS.	Sí
Configurar la función de notificación de correo electrónico.	Sí
Crear plantillas de mapa de auditoría y configurar los mapas de pista de auditoría del proyecto y de la estación de trabajo.	Sí
Activar la función de suma de comprobación para los archivos wiff.	Sí
Tareas comunes	
Añadir nuevos proyectos.	Sí

Instalación de SCIEX OS

Antes de instalar SCIEX OS, lea estos documentos, que están disponibles en el DVD de instalación del software o el paquete de descarga web: *Guía de instalación del software* y *Notas de la versión*. Asegúrese de comprender la diferencia entre un ordenador de procesamiento y un ordenador de adquisición y, a continuación, lleve a cabo la secuencia de instalación correspondiente.

Requisitos del sistema

Para ver los requisitos mínimos de instalación, consulte el documento *Guía de instalación del software*.

Opciones de auditoría predefinidas

Para ver una descripción de los mapas de auditoría instalados, consulte la sección Plantillas del mapa de auditoría instaladas. Tras la instalación, el administrador del software SCIEX OS puede crear mapas de auditoría personalizados y asignar un mapa de auditoría diferente en el espacio de trabajo Configuration.

Configuración del modo de seguridad

En esta sección se describen las opciones de Security Mode que figuran en la página User Management del espacio de trabajo Configuration.

Integrated Mode: En el modo integrado, si el usuario con sesión iniciada en Windows se ha definido como usuario en el software, dicho usuario tiene acceso a SCIEX OS.

Integrated Mode: En el modo integrado, si el usuario con sesión iniciada en Windows se ha definido como usuario en el software, dicho usuario tiene acceso al software .

Mixed Mode: En el modo mixto, los usuarios inician sesión en Windows y en el software por separado. Las credenciales que se usan para iniciar sesión en Windows no tienen que ser las mismas que las utilizadas para iniciar sesión en . Utilice este modo para permitir que un grupo de usuarios inicie sesión en Windows con el mismo conjunto de credenciales, pero que se requiera a cada usuario que inicie sesión en el software con credenciales exclusivas. Se puede asignar una función especial a dichas credenciales exclusivas del mismo modo que en el modo integrado.

Si se selecciona el modo mixto, están disponibles las funciones de bloqueo de pantalla y cierre de sesión automático.

Screen Lock and Auto Logoff: por motivos de seguridad, se puede configurar el bloqueo de la pantalla del ordenador tras un periodo de tiempo de inactividad definido. Asimismo, se puede establecer un temporizador de cierre de sesión automático para que el software se cierre después de que haya estado bloqueado durante un periodo de tiempo definido. Las funciones de bloqueo de la pantalla y cierre de sesión automático solo están disponibles en el modo mixto.

Nota: Cuando la pantalla se bloquea, la adquisición y el procesamiento continúan. El inicio de sesión automático no tendrá lugar si hay procesamiento en curso o si no se ha guardado la tabla de resultados. Cuando se cierra la sesión del usuario mediante el cierre de sesión forzado, todo el procesamiento se detiene y se pierden todos los datos que no se han guardado. La adquisición continúa después de que el usuario haya cerrado sesión automática o manualmente.

Security Notification: el software se puede configurar para enviar automáticamente una notificación por correo electrónico tras un número configurable de errores de inicio de sesión en un periodo de tiempo configurable con el fin de advertir sobre intentos de acceso al

sistema por parte de usuarios no autorizados. El número de errores de inicio de sesión puede ser de 3 a 7 y el periodo de tiempo de 5 minutos a 24 horas.

Nota: En el caso de grupos de trabajo administrados con el software Central Administrator Console (CAC), no se puede gestionar el modo de seguridad con SCIEX OS.

Selección del modo de seguridad

1. Abra el espacio de trabajo Configuration.
2. Haga clic en **User Management**.
3. Haga clic en la pestaña **Security Mode**.
4. Seleccione **Integrated Mode** o **Mixed Mode**. Consulte la sección Configuración del modo de seguridad.
5. Haga clic en **Save**.
   Se muestra un cuadro de diálogo de confirmación.
6. Haga clic en **OK**.

Configuración de las opciones de seguridad de la estación de trabajo (modo mixto)

Procedimientos de condiciones previas
• Establezca el modo de seguridad en el modo mixto. Consulte la sección Configuración del modo de seguridad.

Si se selecciona el modo mixto, se pueden configurar las funciones de bloqueo de pantalla y cierre de sesión automático.

1. Abra el espacio de trabajo Configuration.
2. Haga clic en **User Management**.
3. Abra la pestaña Security Mode.
4. Para configurar la función de bloqueo de pantalla, siga estos pasos:
   a. Seleccione **Screen Lock**.
   b. En el campo **Wait**, especifique una cantidad de tiempo, en minutos.
      Si la estación de trabajo está inactiva durante este período de tiempo, entonces se bloquea automáticamente. El usuario con sesión iniciada puede desbloquear la estación de trabajo introduciendo las credenciales correctas, o bien el administrador puede cerrar la sesión del usuario.
5. Para configurar la función de cierre de sesión automático, siga estos pasos:
   a. Seleccione **Auto Logoff**.
   b. En el campo **Wait**, especifique una cantidad de tiempo, en minutos. Si la estación de trabajo se bloquea durante ese tiempo, ya sea automática o manualmente,

se cierra la sesión del usuario con sesión iniciada en ese momento. Todo el procesamiento se detiene. Sin embargo, la adquisición continúa.

6. Haga clic en **Save**.
   Se abre un cuadro de diálogo de confirmación.
7. Haga clic en **OK**.

Configuración de la notificación por correo electrónico (modo mixto)

Procedimientos de condiciones previas
• Establezca el modo de seguridad en el modo mixto. Consulte la sección: Configuración del modo de seguridad.

El software se puede configurar para que envíe un mensaje de correo electrónico tras producirse un número configurable de errores de inicio de sesión en un periodo de tiempo configurable. El número de errores de inicio de sesión puede ser de 3 a 7 y el periodo de tiempo de 5 minutos a 24 horas.

El ordenador en el que se instale el software debe poder comunicarse con un servidor SMTP con un puerto abierto.

1. Abra el espacio de trabajo Configuration.
2. Haga clic en **User Management**.
3. Abra la pestaña Security Mode.
4. Seleccione la casilla **Send e-mail messages after** y, a continuación, especifique el número de errores de inicio de sesión en el periodo de tiempo concreto (en minutos) a partir del cual se generará una notificación por correo electrónico.

   Sugerencia: Para desactivar la notificación, desmarque la casilla **Send e-mail messages after**.

5. En el campo **SMTP Server**, escriba el nombre del servidor SMTP.

   Nota: La cuenta SMTP enviará un correo al servidor de correo electrónico. El servidor SMTP se define en la aplicación de correo electrónico corporativa.

6. En el campo **Port Number**, escriba el nombre del puerto abierto.
   Haga clic en **Apply Default** para insertar el número de puerto predeterminado (25).
7. En el campo **To**, escriba la dirección de correo electrónico a la que se debe enviar el mensaje. Por ejemplo: nombreusuario@dominio.com.
8. En el campo **From**, escriba la dirección de correo electrónico que se debe mostrar en el campo **From** del mensaje.
9. En el campo **Subject**, escriba el asunto del mensaje.
10. En el campo **Message**, escriba el texto que se debe incluir en el cuerpo del mensaje.

11. Haga clic en **Save**.
    Se abre un diálogo de confirmación.
12. Haga clic en **OK**.
13. Para comprobar la configuración, haga clic en **Send Test Mail**.

Configuración del acceso al software SCIEX OS

Antes de configurar la seguridad, realice lo siguiente:

- Elimine todos los usuarios y grupos de usuarios innecesarios, por ejemplo, el replicador, el usuario avanzado y el operador con privilegios de copia de seguridad del ordenador local y la red.

  Nota: Cada ordenador SCIEX está configurado con una cuenta de administrador local, **abservice**. El servicio técnico y la asistencia técnica de SCIEX usan esta cuenta para instalar el sistema, realizar su mantenimiento y ofrecer asistencia. No elimine ni desactive esta cuenta. Si es necesario eliminar o desactivar la cuenta, prepare un plan alternativo para acceder a SCIEX y comuníquelo a su representante del servicio técnico.

- Agregue grupos de usuarios que contengan grupos con tareas no administrativas asignadas.
- Configure los permisos del sistema.
- Cree los procedimientos y directivas de cuentas correspondientes para los usuarios en la directiva de grupo.

Consulte la documentación de Windows para obtener más información sobre los temas siguientes:

- Usuarios y grupos, y usuarios de Active Directory
- Directivas de bloqueo de cuentas y contraseñas para cuentas de usuario.
- Directiva de derechos del usuario

Si los usuarios trabajan en un entorno de Active Directory, la configuración de la directiva de grupo de Active Directory afectará a la seguridad del ordenador. Revise las directivas de grupo con el administrador de Active Directory como parte de una implementación integral de SCIEX OS.

Permisos para SCIEX OS

Figura 4-1: Página User Management

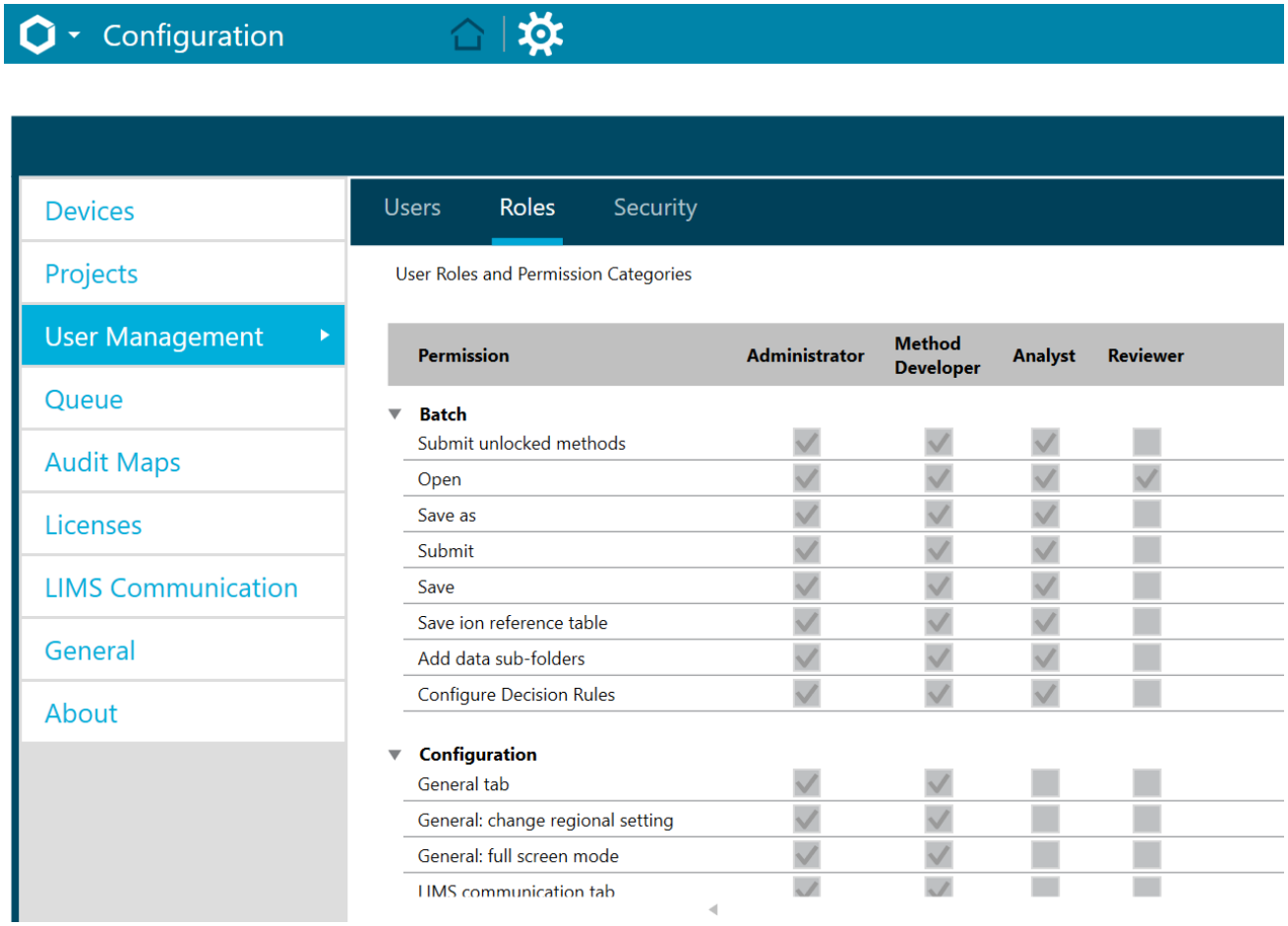


Tabla 4-3: Permisos

Permiso	Descripción
Batch (Lote)	
Submit unlocked methods	(Enviar métodos desbloqueados) Permite a los usuarios enviar lotes que contienen métodos desbloqueados.
Open	(Abrir) Permite que los usuarios abran los lotes existentes.
Save as	(Guardar como) Permite a los usuarios guardar lotes con un nuevo nombre.
Submit	(Enviar) Permite que los usuarios envíen lotes.
Save	(Guardar) Permite a los usuarios guardar un lote, sobrescribiendo el contenido existente.
Save ion reference table	(Guardar la tabla de iones de referencia) Permite a los usuarios editar la tabla de iones de referencia.

Tabla 4-3: Permisos (continuación)

Permiso	Descripción
Add data sub-folders	(Añadir subcarpetas de datos) Permite a los usuarios crear subcarpetas para almacenar los datos.
Configure Decision Rules	(Configurar reglas de decisión) Permite a los usuarios añadir y cambiar reglas de decisión.
Configuration (Configuración)	
General tab	(Pestaña General) Permite a los usuarios abrir la página General en el espacio de trabajo Configuration.
General: change regional setting	(General: cambiar la configuración regional) Permite a los usuarios aplicar la configuración regional actual del sistema a SCIEX OS.
General: full screen mode	(General: modo de pantalla completa) Permite a los usuarios habilitar y deshabilitar el modo de pantalla completa.
General: Stop Windows services	(General: detener servicios de Windows) Permite que los usuarios habiliten o deshabiliten la opción **Windows Settings**.
LIMS communication tab	(Pestaña Comunicación LIMS) Permite a los usuarios abrir la página LIMS Communication en el espacio de trabajo Configuration.
Audit maps tab	(Pestaña Mapas de auditoría) Permite a los usuarios abrir la página Audit Maps en el espacio de trabajo Configuration.
Queue tab	(Pestaña Cola) Permite a los usuarios abrir la página Queue en el espacio de trabajo Configuration.
Queue: instrument idle time	(Cola: tiempo de inactividad del instrumento) Permite a los usuarios establecer el tiempo de inactividad del instrumento.
Queue: max number of acquired samples	(Cola: número máximo de muestras adquiridas) Permite a los usuarios establecer el número máximo permitido de muestras adquiridas.
Queue: other queue settings	(Cola: otros ajustes de la cola) Permite a los usuarios configurar otros ajustes de la cola.
Projects tab	(Pestaña Proyectos) Permite a los usuarios abrir la página Projects en el espacio de trabajo Configuration.
Projects: create project	(Proyectos: crear proyecto) Permite a los usuarios crear proyectos.
Projects: apply an audit map template to an existing project	(Proyectos: aplicar una plantilla de mapa de auditoría a un proyecto existente) Permite a los usuarios aplicar un mapa de auditoría a un proyecto.

Tabla 4-3: Permisos (continuación)

Permiso	Descripción
Projects: create root directory	(Proyectos: crear directorio principal) Permite a los usuarios crear un directorio principal para almacenar proyectos.
Projects: set current root directory	(Proyectos: establecer directorio principal actual) Permite a los usuarios cambiar el directorio principal de un proyecto.
Projects: specify network credentials	(Proyectos: especificar credenciales de red) Permite a los usuarios especificar una cuenta de red segura (SNA) que se usará durante la adquisición de red si el usuario que ha iniciado sesión no tiene acceso al recurso de red.
Projects: Enable checksum writing for wiff data creation	(Proyectos: activar la escritura de sumas de comprobación para la creación de datos wiff) Permite a los usuarios configurar el software para escribir sumas de comprobación en archivos de datos wiff.
Projects: clear root directory	(Proyectos: borrar directorio raíz) Permite a los usuarios eliminar un directorio raíz de la lista.
Devices tab	(Pestaña Dispositivos) Permite a los usuarios abrir la página Devices en el espacio de trabajo Configuration.
User management tab	(Pestaña Administración de usuarios) Permite a los usuarios abrir la página User Management en el espacio de trabajo Configuration.
Force user logoff	(Forzar cierre de sesión del usuario) Permite a los usuarios forzar el cierre de sesión de un usuario que tiene una sesión iniciada en SCIEX OS. Permite a los usuarios forzar el cierre de sesión de un usuario que tiene una sesión iniciada en el software SCIEX OS.
Event Log (Registro de eventos)	
Access event log workspace	(Acceder al espacio de trabajo del registro de eventos) Permite a los usuarios abrir el espacio de trabajo Event Log.
Archive log	(Registro de archivo) Permite a los usuarios archivar el registro de eventos.
Audit Trail (Pista de auditoría)	
Access audit trail workspace	(Acceder al espacio de trabajo de la pista de auditoría) Permite a los usuarios abrir el espacio de trabajo Audit Trail.
View active audit map	(Ver el mapa de auditoría activo) Permite a los usuarios ver el mapa de auditoría activo para una estación de trabajo o un proyecto en el espacio de trabajo de pistas de auditoría.
Print/Export audit trail	(Imprimir/exportar la pista de auditoría) Permite a los usuarios imprimir o exportar la pista de auditoría.

Tabla 4-3: Permisos (continuación)

Permiso	Descripción
CAC Server (Servidor CAC) (solo CAC)	
Manage Workgroups	(Gestionar grupos de trabajo) Permite que los usuarios creen y gestionen grupos de trabajo en el espacio de trabajo de administración de usuarios.
Manage Workgroups Projects	(Gestionar proyectos de grupos de trabajo) Permite que los usuarios creen gestionen grupos de trabajo en el espacio de trabajo de administración de usuarios.
Data Acquisition Panel (Panel Adquisición de datos)	
Start	(Iniciar) Permite a los usuarios iniciar la adquisición en el panel Data Acquisition.
Stop	(Detener) Permite a los usuarios detener la adquisición en el panel Data Acquisition.
Save	(Guardar) Permite a los usuarios guardar los datos adquiridos con un nombre de archivo diferente en el panel Data Acquisition.
MS & LC Method (Método de MS y LC)	
Access method workspace	(Acceder al espacio de trabajo de métodos) Permite a los usuarios abrir los espacios de trabajo MS Method y LC Method.
New	(Nuevo) Permite a los usuarios crear métodos de MS y LC.
Open	(Abrir) Permite a los usuarios abrir métodos de MS y LC.
Save	(Guardar) Permite a los usuarios guardar un método, sobrescribiendo el contenido existente.
Save as	(Guardar como) Permite a los usuarios guardar métodos con un nuevo nombre.
Lock/Unlock method	(Bloquear/desbloquear método) Permite a los usuarios bloquear métodos, para evitar su edición, y desbloquearlos.
Queue (Cola)	
Manage	(Administrar) Permite a los usuarios abrir el espacio de trabajo Queue.
Start/Stop	(Iniciar/Detener) Permite a los usuarios iniciar o detener la cola.
Print	(Imprimir) Permite que los usuarios impriman la cola.
Library (Biblioteca)	

Tabla 4-3: Permisos (continuación)

Permiso	Descripción
Access library workspace	(Acceder al espacio de trabajo de bibliotecas) Permite a los usuarios abrir el espacio de trabajo Library. No aplicable al flujo de cuantificación.
CAC settings (Cliente CAC)	
Enable Central Administration	(Habilitar administración centralizada) Permite que los usuarios configuren SCIEX OS para usar la administración centralizada con el software Central Administrator Console (CAC).
MS Tune (Ajuste de MS)	
Access MS Tune workspace	(Acceder al espacio de trabajo MS Tune) Permite a los usuarios abrir el espacio de trabajo MS Tune.
Advanced MS tuning	(Ajuste de MS avanzado) (Sistemas X500 QTOF) Permite a los usuarios acceder a las opciones de ajuste avanzado, entre otras, Detector Optimization, Positive and Negative Q1 Unit Tuning, Positive and Negative TOF MS Tuning y Positive and Negative Q1 High Tuning.
Advanced troubleshooting	(Resolución de problemas avanzados) Permite a los usuarios abrir el cuadro de diálogo Advanced Troubleshooting.
Quick status check	(Comprobación rápida del estado) (Sistemas X500 QTOF) Permite a los usuarios realizar comprobaciones rápidas del estado positivo y negativo.
Restore instrument data	(Restauración de datos del instrumento) Permite a los usuarios restaurar configuraciones de ajustes guardadas previamente.
Explorer (Explorador)	
Access Explorer workspace	(Acceder al espacio de trabajo Explorer) Permite a los usuarios abrir el espacio de trabajo Explorer.
Export	(Exportar) Permite a los usuarios exportar datos del espacio de trabajo Explorer.
Print	(Imprimir) Permite a los usuarios imprimir datos en el espacio de trabajo Explorer.
Options	(Opciones) Permite a los usuarios modificar las opciones para el espacio de trabajo Explorer.
Recalibrate	(Recalibrar) Permite a los usuarios recalibrar las muestras y los espectros en el espacio de trabajo Explorer. No aplicable al flujo de cuantificación.

Tabla 4-3: Permisos (continuación)

Permiso	Descripción
Analytics (Análisis)	
New results	(Resultados nuevos) Permite a los usuarios crear tablas de resultados.
Create processing method	(Crear método de procesamiento) Permite a los usuarios crear métodos de procesamiento.
Modify processing method	(Modificar método de procesamiento) Permite a los usuarios modificar métodos de procesamiento.
Allow Export and Create Report of unlocked Results Table	(Permitir exportar y crear informes de tabla de resultados sin bloquear) Permite a los usuarios exportar o generar un informe a partir de una tabla de resultados, si la tabla no está bloqueada.
Save results for Automation Batch	(Guardar resultados para lote de automatización) Permite guardar las tablas de resultados creadas automáticamente en el espacio de trabajo Batch. Este permiso es necesario para el procesamiento automático durante la adquisición.
Change default quantitation method integration algorithm	(Cambiar algoritmo predeterminado de integración de métodos de cuantificación) Permite a los usuarios cambiar el algoritmo de integración en la configuración predeterminada del proyecto.
Change default quantitation method integration parameters	(Cambiar parámetros predeterminados de integración de métodos de cuantificación) Permite a los usuarios cambiar los parámetros de integración en la configuración predeterminada del proyecto.
Enable project modified peak warning	(Activar advertencia de pico modificado en proyecto) Permite a los usuarios habilitar la advertencia de pico modificado para un proyecto.
Add samples	(Agregar muestras) Permite a los usuarios agregar muestras a una tabla de resultados.
Remove selected samples	(Eliminar muestras seleccionadas) Permite a los usuarios eliminar muestras de una tabla de resultados.
Export, import, or remove external calibration	(Exportar, importar o eliminar calibración externa) Permite a los usuarios exportar, importar o eliminar calibraciones externas.
Modify sample name	(Modificar nombre de la muestra) Permite a los usuarios modificar el nombre de la muestra en la tabla de resultados.
Modify sample type	(Modificar tipo de muestra) Permite a los usuarios modificar el tipo de muestra, como estándar, control de calidad (QC) o desconocido, en la tabla de resultados.

Tabla 4-3: Permisos (continuación)

Permiso	Descripción
Modify sample ID	(Modificar ID de muestra) Permite a los usuarios modificar el ID de la muestra en la tabla de resultados.
Modify actual concentration	(Modificar concentración real) Permite a los usuarios modificar la concentración real de las muestras Standard y QC en la tabla de resultados.
Modify dilution factor	(Modificar factor de dilución) Permite a los usuarios modificar el factor de dilución en la tabla de resultados.
Modify comment fields	(Modificar campos de comentarios) Permite a los usuarios modificar los campos de comentarios. • Component Comment • IS Comment • IS Peak Comment • Peak Comment • Sample Comment
Enable manual integration	(Habilitar integración manual) Permite a los usuarios realizar la integración manual.
Set peak to Not Found	(Establecer pico como no encontrado) Permite a los usuarios establecer un pico como **Not Found**.
Include or exclude a peak from the Results Table	(Incluir o excluir un pico de la tabla de resultados) Permite a los usuarios incluir y excluir picos de la tabla de resultados.
Regression options	(Opciones de regresión) Permite a los usuarios cambiar las opciones de regresión en el panel Calibration Curve.
Modify Results Table integration parameters for a single chromatogram	(Modificar parámetros de integración de la tabla de resultados para un único cromatograma) Permite a los usuarios cambiar los parámetros de integración para un único cromatograma en el panel Peak Review.
Modify quantitation method for the Results Table component	(Modificar método de cuantificación para el componente de la tabla de resultados) Permite a los usuarios seleccionar un método de procesamiento diferente para un componente en el panel Peak Review con la opción **Update Processing Method for Component**.
Create metric plot new settings	(Crear configuración nueva para el gráfico de métricas) Permite a los usuarios crear nuevos gráficos de métricas y cambiar la configuración.
Add custom columns	(Agregar columnas personalizadas) Permite a los usuarios agregar columnas personalizadas a la tabla de resultados.

Tabla 4-3: Permisos (continuación)

Permiso	Descripción
Set peak review title format	(Definir formato del título de la revisión de picos) Permite a los usuarios cambiar el título de la revisión de picos.
Remove custom column	(Eliminar columna personalizada) Permite a los usuarios eliminar columnas personalizadas de la tabla de resultados.
Results Table display settings	(Configurar visualización de la tabla de resultados) Permite a los usuarios personalizar las columnas mostradas en la tabla de resultados.
Lock Results Table	(Bloquear tabla de resultados) Permite a los usuarios bloquear una tabla de resultados para evitar su edición.
Unlock Results Table	(Desbloquear tabla de resultados) Permite a los usuarios desbloquear una tabla de resultados para permitir su edición.
Mark Results file as reviewed and save	(Marcar archivo de resultados como revisado y guardar) Permite a los usuarios marcar una tabla de resultados como revisada y guardarla.
Modify report template	(Modificar plantilla de informe) Permite a los usuarios cambiar las plantillas de informes.
Transfer results to LIMS	(Transferir resultados a LIMS) Permite a los usuarios cargar resultados en un sistema de gestión de la información del laboratorio (LIMS).
Modify barcode column	(Modificar columna de código de barras) Permite a los usuarios cambiar la columna **Barcode** en una tabla de resultados.
Change comparison sample assignment	(Cambiar la asignación de muestra de comparación) Permite a los usuarios cambiar la muestra de comparación especificada en la columna **Comparison** de la tabla de resultados.
Add the MSMS spectra to library	(Agregar espectros de MSMS a la biblioteca) Permite a los usuarios agregar los espectros MS/MS seleccionados a una biblioteca. No aplicable al flujo de cuantificación.
Project default settings	(Configuración predeterminada del proyecto) Permite a los usuarios cambiar las configuraciones cuantitativa y cualitativa predeterminadas del proyecto.
Create report in all formats	(Crear informes en todos los formatos) Permite a los usuarios generar informes en todos los formatos. Los usuarios sin permiso solo pueden generar informes en formato PDF.

Tabla 4-3: Permisos (continuación)

Permiso	Descripción
Edit flagging criteria parameters	(Editar parámetros de criterios de marcado) Permite a los usuarios cambiar los parámetros de marcado en un método de procesamiento.
Automatic outlier removal parameter change	(Cambio del parámetro de eliminación automática de valores atípicos) Permite a los usuarios cambiar los parámetros para la eliminación automática de valores atípicos.
Enable automatic outlier removal	(Habilitar eliminación automática de valores atípicos) Permite a los usuarios cambiar el método de procesamiento para activar la función de eliminación automática de valores atípicos.
Update processing method via FF/LS	(Actualizar método de procesamiento a través de FF/LS) Permite a los usuarios actualizar los métodos de procesamiento con Formula Finder y Library Search. No aplicable al flujo de cuantificación.
Update results via FF/LS	(Actualizar resultados a través de FF/LS) Permite a los usuarios actualizar los resultados con Formula Finder y Library Search. No aplicable al flujo de cuantificación.
Enable grouping by adducts functionality	(Activar la función de agrupamiento por aducción) Permite a los usuarios actualizar el método de procesamiento para activar la función de agrupamiento por aducción.
Browse for files	(Examinar archivos) Permite a los usuarios buscar archivos fuera de la carpeta de datos local.
Enable standard addition	(Activar adición de patrón) Permite a los usuarios actualizar el método de procesamiento para activar la función de adición de patrón.
Set Manual Integration Percentage Rule	(Establecer regla de porcentaje de integración manual) Permite a los usuarios cambiar el parámetro **Manual Integration %**.

Acerca de los usuarios y las funciones

En SCIEX OS, el administrador puede añadir usuarios y grupos de Windows a la base de datos de administración de usuarios para SCIEX OS. Para acceder al software, los usuarios deben estar definidos en la base de datos de administración de usuarios o deben ser miembros de un grupo definido en la base de datos.

A los usuarios se les puede asignar una o más de las funciones predefinidas que se describen en la tabla mostrada a continuación o también funciones personalizadas si es necesario. Las funciones determinan las funcionalidades a las que tienen acceso los usuarios. Las funciones predefinidas no se pueden eliminar ni tampoco modificar sus permisos.

Nota: En el caso de grupos de trabajo administrados con el software Central Administrator Console (CAC), las páginas User Management son de solo lectura.

Tabla 4-4: Funciones predefinidas

Función	Tareas típicas
Administrator (Administrador)	• Administra el sistema. • Configura la seguridad.
Method Developer (Desarrollador de método)	• Crea métodos. • Ejecuta lotes. • Analiza los datos que va a utilizar el usuario final.
Analyst (Analista)	• Ejecuta lotes. • Analiza los datos que va a utilizar el usuario final.
Reviewer (Revisor)	• Revisa los datos. • Revisa las pistas de auditoría. • Revisa los resultados de cuantificación.

Tabla 4-5: Permisos predeterminados

Permiso	Administrador	Desarrollador de método	Analista	Revisor
Batch (Lote)				
Submit unlocked methods (Enviar métodos desbloqueados)	✓	✓	✓	×
Open (Abrir)	✓	✓	✓	✓
Save as (Guardar como)	✓	✓	✓	×
Submit (Enviar)	✓	✓	✓	×
Save (Guardar)	✓	✓	✓	×
Save ion reference table (Guardar la tabla de iones de referencia)	✓	✓	✓	×
Add data sub-folders (Añadir subcarpetas de datos)	✓	✓	✓	×

Tabla 4-5: Permisos predeterminados (continuación)

Permiso	Administrador	Desarrollador de método	Analista	Revisor
Configure Decision Rules (Configurar reglas de decisión)	✓	✓	✓	×
Configuration (Configuración)				
General tab (pestaña General)	✓	✓	×	×
General: change regional setting (General: cambiar configuración regional)	✓	✓	×	×
General: full screen mode (General: modo de pantalla completa)	✓	✓	×	×
General: Stop Windows services (General: detener servicios de Windows)	✓	×	×	×
LIMS communication tab (pestaña Comunicación LIMS)	✓	✓	×	×
Audit maps tab (pestaña Mapas de auditoría)	✓	×	×	×
Queue tab (pestaña Cola)	✓	✓	✓	✓
Queue: instrument idle time (Cola: tiempo de inactividad del instrumento)	✓	✓	×	×
Queue: max number of acquired samples (Cola: número máximo de muestras adquiridas)	✓	✓	×	×
Queue: other queue settings (Cola: otros ajustes de la cola)	✓	✓	×	×

Tabla 4-5: Permisos predeterminados (continuación)

Permiso	Administrador	Desarrollador de método	Analista	Revisor
Projects tab (pestaña Proyectos)	✓	✓	✓	✓
Projects: create project (Proyectos: crear proyecto)	✓	✓	✓	×
Projects: apply an audit map template to an existing project (Proyectos: aplicar una plantilla de mapa de auditoría a un proyecto existente)	✓	×	×	×
Projects: create root directory (Proyectos: crear directorio principal)	✓	×	×	×
Projects: set current root directory (Proyectos: establecer directorio principal actual)	✓	×	×	×
Projects: specify network credentials (Proyectos: especificar credenciales de red)	✓	×	×	×
Projects: Enable checksum writing for wiff1 data creation (Proyectos: activar la escritura de sumas de comprobación para la creación de datos wiff1)	✓	×	×	×
Projects: clear root directory (Proyectos: crear directorio raíz)	✓	×	×	×
Devices tab (pestaña Dispositivos)	✓	✓	✓	×

Tabla 4-5: Permisos predeterminados (continuación)

Permiso	Administrador	Desarrollador de método	Analista	Revisor
User management tab (pestaña Gestión de usuarios)	✓	×	×	×
Force user logoff (Forzar cierre de sesión del usuario)	✓	×	×	×
Event Log (Registro de eventos)				
Access event log workspace (Acceder al espacio de trabajo del registro de eventos)	✓	✓	✓	✓
Archive log (Registro de archivos)	✓	✓	✓	✓
Audit Trail (Pista de auditoría)				
Access audit trail workspace (Acceder al espacio de trabajo de pistas de auditoría)	✓	✓	✓	✓
View active audit map (Ver el mapa de auditoría activo)	✓	✓	✓	✓
Print/Export audit trail (Imprimir/exportar la pista de auditoría)	✓	✓	✓	✓
Data Acquisition Panel (Panel Adquisición de datos)				
Start (Iniciar)	✓	✓	✓	×
Stop (Detener)	✓	✓	✓	×
Save (Guardar)	✓	✓	✓	×
MS & LC Method (Método de MS y LC)				
Access method workspace (Acceder al espacio de trabajo de métodos)	✓	✓	✓	✓
New (Nuevo)	✓	✓	×	×
Open (Abrir)	✓	✓	✓	✓

Tabla 4-5: Permisos predeterminados (continuación)

Permiso	Administrador	Desarrollador de método	Analista	Revisor
Save (Guardar)	✓	✓	×	×
Save as (Guardar como)	✓	✓	×	×
Lock/Unlock method (Método de bloqueo/ desbloqueo)	✓	✓	×	×
Queue (Cola)				
Manage (Administrar)	✓	✓	✓	×
Start/Stop (Iniciar/ Detener)	✓	✓	✓	×
Print (Impresión)	✓	✓	✓	✓
Library (Biblioteca)				
Access library workspace (Acceder al espacio de trabajo de bibliotecas)	✓	✓	✓	✓
CAC settings (Cliente CAC)				
Enable Central Administration (Activar administración centralizada)	✓	×	×	×
MS Tune (Ajuste de MS)				
Access MS Tune workspace (Acceder al espacio de trabajo MS Tune)	✓	✓	✓	×
Advanced MS Tuning (Ajuste de MS avanzado)	✓	✓	×	×
Advanced troubleshooting (Resolución de problemas avanzados)	✓	✓	×	×
Quick status check (Comprobación rápida del estado)	✓	✓	✓	×

Tabla 4-5: Permisos predeterminados (continuación)

Permiso	Administrador	Desarrollador de método	Analista	Revisor
Restore instrument data (Restauración de datos del instrumento)	✓	✓	×	×
Explorer (Explorador)				
Access explorer workspace (Acceder al espacio de trabajo Explorer)	✓	✓	✓	✓
Export (Exportar)	✓	✓	✓	×
Print (Impresión)	✓	✓	✓	×
Options (Opciones)	✓	✓	✓	×
Recalibrate (Recalibrar)	✓	✓	×	×
Analytics (Análisis)				
New results (Resultados nuevos)	✓	✓	✓	×
Create processing method (Crear método de procesamiento)	✓	✓	✓	×
Modify processing method (Modificar método de procesamiento)	✓	✓	×	×
Allow Export and Create Report of unlocked Results Table (Permitir exportar y crear informes de tabla de resultados sin bloquear)	✓	×	×	×
Save results for Automation Batch (Guardar resultados para el lote de automatización)	✓	✓	✓	×

Tabla 4-5: Permisos predeterminados (continuación)

Permiso	Administrador	Desarrollador de método	Analista	Revisor
Change default quantitation method integration algorithm (Cambiar algoritmo predeterminado de integración de métodos de cuantificación)	✓	✓	×	×
Change default quantitation method integration parameters (Cambiar parámetros predeterminados de integración de métodos de cuantificación)	✓	✓	×	×
Enable project modified peak warning (Activar advertencia de pico modificado en proyecto)	✓	×	×	×
Add samples (Agregar muestras)	✓	✓	✓	×
Remove selected samples (Eliminar muestras seleccionadas)	✓	✓	✓	×
Export, import, or remove external calibration (Exportar, importar o eliminar calibración externa)	✓	✓	✓	×
Modify sample name (Modificar nombre de la muestra)	✓	✓	✓	×
Modify sample type (Modificar tipo de la muestra)	✓	✓	✓	×

Tabla 4-5: Permisos predeterminados (continuación)

Permiso	Administrador	Desarrollador de método	Analista	Revisor
Modify sample ID (Modificar ID de la muestra)	✓	✓	✓	×
Modify actual concentration (Modificar concentración real)	✓	✓	✓	×
Modify dilution factor (Modificar factor de dilución)	✓	✓	✓	×
Modify comment fields (Modificar los campos de comentarios)	✓	✓	✓	×
Enable manual integration (Activar integración manual)	✓	✓	✓	×
Set peak to not found (Establecer pico como no encontrado)	✓	✓	✓	×
Include or exclude a peak from the results table (Incluir o excluir un pico de la tabla de resultados)	✓	✓	✓	×
Regression options (Opciones de regresión)	✓	✓	✓	×
Modify results table integration parameters for a single chromatogram (Modificar parámetros de integración de la tabla de resultados para un único cromatograma)	✓	✓	✓	×

Tabla 4-5: Permisos predeterminados (continuación)

Permiso	Administrador	Desarrollador de método	Analista	Revisor
Modify quantitation method for the results table component (Modificar método de cuantificación para el componente de la tabla de resultados)	✓	✓	✓	×
Create metric plot new settings (Crear configuración nueva para el gráfico de métricas)	✓	✓	✓	✓
Add custom columns (Agregar columnas personalizadas)	✓	✓	✓	×
Set peak review title format (Definir formato del título de la revisión de picos)	✓	×	×	×
Remove custom column (Eliminar columnas personalizadas)	✓	✓	×	×
Results table display settings (Configurar visualización de la tabla de resultados)	✓	✓	✓	✓
Lock results table (Bloquear tabla de resultados)	✓	✓	✓	✓
Unlock results table (Desbloquear tabla de resultados)	✓	×	×	×
Mark results file as reviewed and save (Marcar archivo de resultados como revisado y guardar)	✓	×	×	✓

Tabla 4-5: Permisos predeterminados (continuación)

Permiso	Administrador	Desarrollador de método	Analista	Revisor
Modify report template (Modificar plantilla de informe)	✓	✓	×	×
Transfer results to LIMS (Transferir resultados a LIMS)	✓	✓	✓	×
Modify barcode column (Modificar columna de código de barras)	✓	✓	×	×
Change comparison sample assignment (Cambiar la asignación de muestra de comparación)	✓	✓	×	×
Add the MSMS spectra to library (Agregar espectros de MSMS a la biblioteca)	✓	✓	×	×
Project default settings (Configuración predeterminada del proyecto)	✓	✓	×	×
Create report in all formats (Crear informes en todos los formatos)	✓	✓	✓	✓
Edit flagging criteria parameters (Editar parámetros de criterios de marcado)	✓	✓	✓	×
Automatic outlier removal parameter change (Cambio del parámetro de eliminación automática de valores atípicos)	✓	✓	×	×

Tabla 4-5: Permisos predeterminados (continuación)

Permiso	Administrador	Desarrollador de método	Analista	Revisor
Enable automatic outlier removal (Activar eliminación automática de valores atípicos)	✓	✓	✓	×
Update processing method via FF/LS (Actualizar método de procesamiento a través de FF/LS)	✓	✓	×	×
Update results via FF/LS (Actualizar resultados a través de FF/LS)	✓	✓	×	×
Enable grouping by adducts functionality (Activar la función de agrupamiento por aducción)	✓	✓	×	×
Browse for files (Examinar archivos)	✓	✓	✓	✓
Enable standard addition (Activar adición de patrón)	✓	✓	✓	×
Set Manual Integration Percentage Rule (Establecer regla de porcentaje de integración manual)	✓	×	×	×

Gestión de usuarios

Adición de un usuario o grupo

1. Abra el espacio de trabajo Configuration.
2. Abra la página User Management.
3. Abra la pestaña Users.
4. Haga clic en **Add User** ().

Se abre el cuadro de diálogo Select User or Group.

5. Escriba el nombre de un grupo de usuario y haga clic en **OK**.

Sugerencia: Para obtener información sobre el cuadro de diálogo Select User or Group y cómo usarlo, pulse **F1**.

6. Para activar al usuario, asegúrese de seleccionar la casilla **Active user or group**.
7. En el área **Roles**, seleccione una o varias funciones y haga clic en **Save**.

Desactivación de usuarios o grupos

1. Abra el espacio de trabajo Configuration.
2. Abra la página User Management.
3. Abra la pestaña Users.
4. En la lista **User name or group**, seleccione el usuario o grupo que desea desactivar.
5. Desactive la casilla **Active user or group**.
   El software solicita confirmación.
6. Haga clic en **Yes**.

Eliminación de usuarios o grupos

Utilice este procedimiento para eliminar un usuario o grupo del software. Si elimina un usuario o grupo de Windows, el usuario también se debe quitar de SCIEX OS.

1. Abra el espacio de trabajo Configuration.
2. Abra la página User Management.
3. Abra la pestaña Users.
4. En la lista **User name or group**, seleccione el usuario o grupo que desea eliminar.
5. Haga clic en **Delete**.
   El software solicita confirmación.
6. Haga clic en **OK**.

Gestión de funciones

Cambio de funciones asignadas a un usuario o grupo

Utilice este procedimiento para asignar funciones nuevas a un usuario o a un grupo o eliminar las asignaciones de funciones existentes.

1. Abra el espacio de trabajo Configuration.
2. Abra la página User Management.
3. Abra la pestaña Users.
4. En el campo **User name or group**, seleccione el usuario o grupo que desee modificar.

5. Seleccione las funciones que desea asignar al usuario o al grupo y borre las funciones que desea eliminar.
6. Haga clic en **Save**.

Creación de una función personalizada

1. Abra el espacio de trabajo Configuration.
2. Abra la página User Management.
3. Abra la pestaña Roles.
4. Haga clic en **Add Role** ().
   Se abre el cuadro de diálogo Duplicate a User Role.
5. En el campo **Existing user role**, seleccione la función que se va a utilizar como plantilla para la función nueva.
6. Escriba un nombre y una descripción de la función y haga clic en **OK**.
7. Seleccione los privilegios de acceso de la función.
8. Haga clic en **Save All Roles**.
9. Haga clic en **OK**.

Eliminación de una función personalizada

Nota: Si un usuario solo tiene asignada la función que se va a eliminar, el sistema indica que se elimine el usuario además de la función.

1. Abra el espacio de trabajo Configuration.
2. Abra la página User Management.
3. Abra la pestaña Roles.
4. Haga clic en **Delete a Role**.
   Se abre el cuadro de diálogo Delete a User Role.
5. Seleccione la función que desea eliminar y, a continuación, haga clic en **OK**.

Exportación e importación de la configuración de administración de usuarios

La base de datos de administración de usuarios de SCIEX OS se puede exportar e importar. Después de configurar la base de datos de administración de usuarios en un ordenador SCIEX, por ejemplo, expórtela y, a continuación, impórtela en otros ordenadores SCIEX para asegurarse de que la configuración de administración de usuarios sea coherente.

Solo se exportan los usuarios del dominio. Los usuarios locales no se exportan.

Antes de importar la configuración de administración de usuarios, el software realiza automáticamente una copia de seguridad de la configuración actual. El usuario puede restaurar la última copia de seguridad.

Exportación de la configuración de administración de usuarios

1. Abra el espacio de trabajo Configuration.
2. Abra la página User Management.
3. Haga clic en **Advanced** > **Export User Management settings**.
   Se abre el cuadro de diálogo Export User Management Settings.
4. Haga clic en **Browse**.
5. Busque y seleccione la carpeta donde se guardará la configuración y, a continuación, haga clic en **Select Folder**.
6. Haga clic en **Export**.
   Aparecerá un mensaje de confirmación con el nombre del archivo que contiene la configuración exportada.
7. Haga clic en **OK**.

Importación de la configuración de administración de usuarios

1. Abra el espacio de trabajo Configuration.
2. Abra la página User Management.
3. Haga clic en **Advanced** > **Import User Management settings**.
   Se abre el cuadro de diálogo Import User Management Settings.
4. Haga clic en **Browse**.
5. Busque y seleccione el archivo que contiene la configuración que desea importar y, a continuación, haga clic en **Open**.
   El software comprueba que el archivo sea válido.
6. Haga clic en **Import**.
   El software realiza una copia de seguridad de la configuración actual de administración de usuarios e importa la nueva configuración. Se muestra un mensaje de confirmación.
7. Haga clic en **OK**.

Restauración de la configuración de administración de usuarios

Antes de importar la configuración de administración de usuarios, el software realiza una copia de seguridad de la configuración actual. Utilice este procedimiento para restaurar la última copia de seguridad de la configuración de administración de usuarios.

1. Abra el espacio de trabajo Configuration.

2. Abra la página User Management.
3. Haga clic en **Advanced** > **Restore previous settings**.
   Se abre el cuadro de diálogo Restore User Management Settings.
4. Haga clic en **Yes**.
5. Cierre SCIEX OS y vuelva a abrirlo.

Configuración del acceso a proyectos y archivos de proyectos

Utilice las funciones de seguridad de Windows para controlar el acceso a la carpeta `SCIEX OS Data`. De forma predeterminada, los archivos de proyecto se almacenan en la carpeta `SCIEX OS Data`. Para acceder a un proyecto, los usuarios deben tener acceso al directorio principal en el que se almacenan los datos del proyecto. Para obtener más información, consulte la sección Configuración del sistema de seguridad de Windows.

Carpetas de un proyecto

Cada proyecto contiene carpetas en las que se guardan diferentes tipos de archivos. Para obtener más información sobre el contenido de las distintas carpetas, consulte la Tabla 4-6.

Tabla 4-6: Carpetas de un proyecto

Carpeta	Contenido
`\Acquisition Methods`	Contiene los métodos de espectrómetro de masas (MS) y de LC que se han creado en el proyecto. Los métodos de MS tienen la extensión msm, y los métodos de LC tienen la extensión lcm.
`\Audit Data`	Contiene el mapa de auditoría del proyecto y todos los registros de auditoría.
`\Batch`	Contiene todos los archivos de lotes de adquisición que se han guardado. Los lotes de adquisición tienen la extensión bch.
`\Data`	Contiene los archivos de datos de adquisición. Los archivos de datos de adquisición tienen las extensiones wiff y wiff2.
`\Project Information`	Contiene los archivos de configuración predeterminada del proyecto.
`\Quantitation Methods`	Contiene todos los archivos de métodos de procesamiento. Los métodos de procesamiento tienen la extensión qmethod.
`\Quantitation Results`	Contiene todos los archivos de tablas de resultados de cuantificación. Los archivos de tablas de resultados tienen la extensión qsession.

Tipos de archivo del software

Para los tipos de archivo comunes de SCIEX OS, consulte la Tabla 4-7.

Tabla 4-7: Archivos de SCIEX OS

Extensión	Tipo de archivo	Carpeta
atds	• Datos y archivos de pista de auditoría de la estación de trabajo • Configuración de pistas de auditoría de la estación de trabajo • Datos y archivos de pista de auditoría del proyecto • Configuración de pistas de auditoría de proyectos	• Para los proyectos: `<project name>\Audit Data` • Para la estación de trabajo: `C:\ProgramData\SCIEX\Audit Data`
atms	Mapas de auditoría	• Para los proyectos: `<project name>\Audit Data` • Para la estación de trabajo: `C:\ProgramData\SCIEX\Audit Data`
bch	Batch	`Batch`
cset	Configuración de la tabla de resultados	`Project Information`
dad	Archivo de datos de espectrometría de masas	• `Optimization` • `Data`
exml	Configuración predeterminada del proyecto	`Project Information`
journal	Archivos temporales creados por SCIEX OS	Varias carpetas
lcm	Método de LC	`Acquisition Methods`
msm	Método de MS	`Acquisition Methods`
pdf	Formato de documento portátil	—
qlayout	Diseño del espacio de trabajo	— **Nota:** El diseño de espacio de trabajo predeterminado de un proyecto se almacena en la carpeta `Project Information`.

Tabla 4-7: Archivos de SCIEX OS (continuación)

Extensión	Tipo de archivo	Carpeta
qmethod	Método de procesamiento	`Quantitation Methods`
qsession	Tabla de resultados del software Tabla de resultados **Nota:** SCIEX OS solo puede abrir archivos qsession creados con SCIEX OS.	`Quantitation Results`
wiff	Archivo de datos de espectrometría de masas compatible con el software SCIEX OS **Nota:** SCIEX OS genera archivos wiff y wiff2.	`Data`
wiff.scan	Archivo de datos de espectrometría de masas	• `Optimization` • `Data`
wiff2	Archivo de datos de espectrometría de masas generado por SCIEX OS	• `Optimization` • `Data`
xls o xlsx	Hoja de cálculo Excel	`Batch`
xps	Recalibración	`Data\Cal`

Central Administrator Console 5

El software Central Administrator Console (CAC) es una alternativa opcional a la administración local con el software SCIEX OS. El software CAC incluye la gestión y la personalización centralizadas de funciones, usuarios, estaciones de trabajo y grupos de trabajo en una sola aplicación.

En esta sección se describe el software CAC y se explica cómo configurarlo y utilizarlo para gestionar usuarios, proyectos y estaciones de trabajo de manera centralizada.

Nota: Para usar el software CAC y registrar estaciones de trabajo con el servidor, asegúrese de que el software SCIEX OS esté instalado en cada estación de trabajo.

El software CAC está habilitado con la licencia y se puede instalar en cualquier estación de trabajo que admita la versión 3.0 de SCIEX OS y Windows Server 2019.

El software CAC forma parte del paquete de instalación de SCIEX OS. Sin embargo, el software CAC y SCIEX OSno se pueden instalar en la misma estación de trabajo.

Usuarios

Utilice la página User Management para añadir usuarios y grupos de Windows a la base de datos de administración de usuarios para SCIEX OS. El administrador también puede añadir, modificar y eliminar funciones de usuario en la sección de funciones y permisos de usuario. Para acceder al software, los usuarios deben estar definidos en la base de datos de administración de usuarios o deben ser miembros de un grupo definido en la base de datos.

Conjunto de usuarios

Solo los usuarios autorizados pueden iniciar sesión en la estación de trabajo y acceder a SCIEX OS cuando SCIEX OS se administra con el software Central Administrator Console (CAC). Antes de poder añadir usuarios a los grupos de trabajo, hay que añadirlos al conjunto de usuarios.

Adición de un usuario o grupo al Conjunto de usuarios

1. Abra el espacio de trabajo Central Administration.
2. Abra la página User Management.
3. Abra la pestaña User Pool.
4. Haga clic en **Add users to the User Pool** ( ).
   Se abre el cuadro de diálogo Select Users or Groups.
5. Escriba el nombre de un usuario o grupo y haga clic en **OK**.

Sugerencia: Mantenga pulsada la tecla **Ctrl** y, a continuación, haga clic en **OK** para seleccionar varios usuarios o grupos.

Eliminar usuarios o grupos

1. Abra el espacio de trabajo Central Administration.
2. Abra la página User Management.
3. Abra la pestaña User Pool.
4. En el panel derecho, seleccione el usuario o grupo que desee eliminar, y, a continuación, haga clic en **Delete**.
   El software solicita confirmación.
5. Haga clic en **OK**.

Funciones y permisos de usuario

En esta sección se describe la página User Roles and Permissions.

A los usuarios se les puede asignar una o más de las funciones predefinidas que se describen en la tabla mostrada a continuación o también funciones personalizadas si es necesario. Las funciones determinan las funcionalidades a las que tienen acceso los usuarios. Las funciones predefinidas no se pueden eliminar ni tampoco modificar sus permisos.

Tabla 5-1: Funciones predefinidas

Función	Tareas típicas
Administrator (Administrador)	• Administra el sistema. • Configura la seguridad.
Method Developer (Desarrollador de método)	• Crea métodos. • Ejecuta lotes. • Analiza los datos que va a utilizar el usuario final.
Analyst (Analista)	• Ejecuta lotes. • Analiza los datos que va a utilizar el usuario final.
Reviewer (Revisor)	• Revisa los datos. • Revisa las pistas de auditoría. • Revisa los resultados de cuantificación.

Tabla 5-2: Permisos predeterminados

Permiso	Administrador	Desarrollador de método	Analista	Revisor
Batch (Lote)				
Submit unlocked methods (Enviar métodos desbloqueados)	✓	✓	✓	×
Open (Abrir)	✓	✓	✓	✓
Save as (Guardar como)	✓	✓	✓	×
Submit (Enviar)	✓	✓	✓	×
Save (Guardar)	✓	✓	✓	×
Save ion reference table (Guardar la tabla de iones de referencia)	✓	✓	✓	×
Add data sub-folders (Añadir subcarpetas de datos)	✓	✓	✓	×
Configure Decision Rules (Configurar reglas de decisión)	✓	✓	✓	×
Configuration (Configuración)				
General tab (pestaña General)	✓	✓	×	×
General: change regional setting (General: cambiar configuración regional)	✓	✓	×	×
General: full screen mode (General: modo de pantalla completa)	✓	✓	×	×
LIMS communication tab (pestaña Comunicación LIMS)	✓	✓	×	×
General:Stop Windows services(General: detener servicios de Windows)	✓	×	×	×

Tabla 5-2: Permisos predeterminados (continuación)

Permiso	Administrador	Desarrollador de método	Analista	Revisor
Audit maps tab (pestaña Mapas de auditoría)	✓	×	×	×
Queue tab (pestaña Cola)	✓	✓	✓	✓
Queue: instrument idle time (Cola: tiempo de inactividad del instrumento)	✓	✓	×	×
Queue: max number of acquired samples (Cola: número máximo de muestras adquiridas)	✓	✓	×	×
Queue: other queue settings (Cola: otros ajustes de la cola)	✓	✓	×	×
Projects tab (pestaña Proyectos)	✓	✓	✓	✓
Projects: create project (Proyectos: crear proyecto)	✓	✓	✓	×
Projects: apply an audit map template to an existing project (Proyectos: aplicar una plantilla de mapa de auditoría a un proyecto existente)	✓	×	×	×
Projects: create root directory (Proyectos: crear directorio principal)	✓	×	×	×
Projects: set current root directory (Proyectos: establecer directorio principal actual)	✓	×	×	×

Tabla 5-2: Permisos predeterminados (continuación)

Permiso	Administrador	Desarrollador de método	Analista	Revisor
Projects: specify network credentials (Proyectos: especificar credenciales de red)	✓	×	×	×
Projects: Enable checksum writing for wiff1 data creation (Proyectos: activar la escritura de sumas de comprobación para la creación de datos wiff1)	✓	×	×	×
Projects: clear root directory (Proyectos: crear directorio raíz)	✓	×	×	×
Devices tab (pestaña Dispositivos)	✓	✓	✓	×
User management tab (pestaña Gestión de usuarios)	✓	×	×	×
Force user logoff (Forzar cierre de sesión del usuario)	✓	×	×	×
Event Log (Registro de eventos)				
Access event log workspace (Acceder al espacio de trabajo del registro de eventos)	✓	✓	✓	✓
Archive log (Registro de archivos)	✓	✓	✓	✓
Audit Trail (Pista de auditoría)				
Access audit trail workspace (Acceder al espacio de trabajo de pistas de auditoría)	✓	✓	✓	✓
View active audit map (Ver el mapa de auditoría activo)	✓	✓	✓	✓

Tabla 5-2: Permisos predeterminados (continuación)

Permiso	Administrador	Desarrollador de método	Analista	Revisor
Print/Export audit trail (Imprimir/exportar la pista de auditoría)	✓	✓	✓	✓
Data Acquisition Panel (Panel Adquisición de datos)				
Start (Iniciar)	✓	✓	✓	×
Stop (Detener)	✓	✓	✓	×
Save (Guardar)	✓	✓	✓	×
MS & LC Method (Método de MS y LC)				
Access method workspace (Acceder al espacio de trabajo de métodos)	✓	✓	✓	✓
New (Nuevo)	✓	✓	×	×
Open (Abrir)	✓	✓	✓	✓
Save (Guardar)	✓	✓	×	×
Save as (Guardar como)	✓	✓	×	×
Lock/Unlock method (Método de bloqueo/ desbloqueo)	✓	✓	×	×
Queue (Cola)				
Manage (Administrar)	✓	✓	✓	×
Start/Stop (Iniciar/ Detener)	✓	✓	✓	×
Print (Impresión)	✓	✓	✓	✓
Library (Biblioteca)				
Access library workspace (Acceder al espacio de trabajo de bibliotecas)	✓	✓	✓	✓
CAC settings (Cliente CAC)				

Tabla 5-2: Permisos predeterminados (continuación)

Permiso	Administrador	Desarrollador de método	Analista	Revisor
Enable Central Administration (Activar administración centralizada)	✓	×	×	×
MS Tune (Ajuste de MS)				
Access MS Tune workspace (Acceder al espacio de trabajo MS Tune)	✓	✓	✓	×
Advanced MS Tuning (Ajuste de MS avanzado)	✓	✓	×	×
Advanced troubleshooting (Resolución de problemas avanzados)	✓	✓	×	×
Quick status check (Comprobación rápida del estado)	✓	✓	✓	×
Restore instrument data (Restauración de datos del instrumento)	✓	✓	×	×
Analytics (Análisis)				
New results (Resultados nuevos)	✓	✓	✓	×
Create processing method (Crear método de procesamiento)	✓	✓	✓	×
Modify processing method (Modificar método de procesamiento)	✓	✓	×	×

Tabla 5-2: Permisos predeterminados (continuación)

Permiso	Administrador	Desarrollador de método	Analista	Revisor
Allow Export and Create Report of unlocked Results Table (Permitir exportar y crear informes de tabla de resultados sin bloquear)	✓	×	×	×
Save results for Automation Batch (Guardar resultados para el lote de automatización)	✓	✓	✓	×
Change default quantitation method integration algorithm (Cambiar algoritmo predeterminado de integración de métodos de cuantificación)	✓	✓	×	×
Change default quantitation method integration parameters (Cambiar parámetros predeterminados de integración de métodos de cuantificación)	✓	✓	×	×
Enable project modified peak warning (Activar advertencia de pico modificado en proyecto)	✓	×	×	×
Add samples (Agregar muestras)	✓	✓	✓	×
Remove selected samples (Eliminar muestras seleccionadas)	✓	✓	✓	×

Tabla 5-2: Permisos predeterminados (continuación)

Permiso	Administrador	Desarrollador de método	Analista	Revisor
Export, import, or remove external calibration (Exportar, importar o eliminar calibración externa)	✓	✓	✓	×
Modify sample name (Modificar nombre de la muestra)	✓	✓	✓	×
Modify sample type (Modificar tipo de la muestra)	✓	✓	✓	×
Modify sample ID (Modificar ID de la muestra)	✓	✓	✓	×
Modify actual concentration (Modificar concentración real)	✓	✓	✓	×
Modify dilution factor (Modificar factor de dilución)	✓	✓	✓	×
Modify comment fields (Modificar los campos de comentarios)	✓	✓	✓	×
Enable manual integration (Activar integración manual)	✓	✓	✓	×
Set peak to not found (Establecer pico como no encontrado)	✓	✓	✓	×
Include or exclude a peak from the results table (Incluir o excluir un pico de la tabla de resultados)	✓	✓	✓	×
Regression options (Opciones de regresión)	✓	✓	✓	×

Tabla 5-2: Permisos predeterminados (continuación)

Permiso	Administrador	Desarrollador de método	Analista	Revisor
Modify results table integration parameters for a single chromatogram (Modificar parámetros de integración de la tabla de resultados para un único cromatograma)	✓	✓	✓	×
Modify quantitation method for the results table component (Modificar método de cuantificación para el componente de la tabla de resultados)	✓	✓	✓	×
Create metric plot new settings (Crear configuración nueva para el gráfico de métricas)	✓	✓	✓	✓
Add custom columns (Agregar columnas personalizadas)	✓	✓	✓	×
Set peak review title format (Definir formato del título de la revisión de picos)	✓	×	×	×
Remove custom column (Eliminar columnas personalizadas)	✓	✓	×	×
Results table display settings (Configurar visualización de la tabla de resultados)	✓	✓	✓	✓
Lock results table (Bloquear tabla de resultados)	✓	✓	✓	✓

Tabla 5-2: Permisos predeterminados (continuación)

Permiso	Administrador	Desarrollador de método	Analista	Revisor
Unlock results table (Desbloquear tabla de resultados)	✓	×	×	×
Mark results file as reviewed and save (Marcar archivo de resultados como revisado y guardar)	✓	×	×	✓
Modify report template (Modificar plantilla de informe)	✓	✓	×	×
Transfer results to LIMS (Transferir resultados a LIMS)	✓	✓	✓	×
Modify barcode column (Modificar columna de código de barras)	✓	✓	×	×
Change comparison sample assignment (Cambiar la asignación de muestra de comparación)	✓	✓	×	×
Add the MSMS spectra to library (Agregar espectros de MSMS a la biblioteca)	✓	✓	×	×
Project default settings (Configuración predeterminada del proyecto)	✓	✓	×	×
Create report in all formats (Crear informes en todos los formatos)	✓	✓	✓	✓
Edit flagging criteria parameters (Editar parámetros de criterios de marcado)	✓	✓	✓	×

Tabla 5-2: Permisos predeterminados (continuación)

Permiso	Administrador	Desarrollador de método	Analista	Revisor
Automatic outlier removal parameter change (Cambio del parámetro de eliminación automática de valores atípicos)	✓	✓	×	×
Enable automatic outlier removal (Activar eliminación automática de valores atípicos)	✓	✓	✓	×
Update processing method via FF/LS (Actualizar método de procesamiento a través de FF/LS)	✓	✓	×	×
Update results via FF/LS (Actualizar resultados a través de FF/LS)	✓	✓	×	×
Enable grouping by adducts functionality (Activar la función de agrupamiento por aducción)	✓	✓	×	×
Browse for files (Examinar archivos)	✓	✓	✓	✓
Enable standard addition (Activar adición de patrón)	✓	✓	✓	×
Set Manual Integration Percentage Rule (Establecer regla de porcentaje de integración manual)	✓	×	×	×
Explorer (Explorador)				

Tabla 5-2: Permisos predeterminados (continuación)

Permiso	Administrador	Desarrollador de método	Analista	Revisor
Access explorer workspace (Acceder al espacio de trabajo Explorer)	✓	✓	✓	✓
Export (Exportar)	✓	✓	✓	×
Print (Impresión)	✓	✓	✓	×
Options (Opciones)	✓	✓	✓	×
Recalibrate (Recalibrar)	✓	✓	×	×

Añadir una función personalizada

El software Central Administrator Console (CAC) tiene cuatro funciones predefinidas. Si se necesitan más funciones, copie una función existente y asígnele derechos de acceso.

1. Abra el espacio de trabajo Central Administration.
2. Abra la página User Management.
3. Abra la pestaña User Roles and Permissions.
4. Haga clic en **Add Role** ( ).
   Se abre el cuadro de diálogo Duplicate a User Role.
5. En el campo **Existing user role**, seleccione la función que se va a utilizar como plantilla para la función nueva.
6. Escriba un nombre y una descripción de la función y haga clic en **OK**.
   La nueva función se muestra en la ventana User Roles and Permission Categories.
7. Seleccione los privilegios de acceso para la función marcando las casillas correspondientes.
8. Haga clic en **Save All Roles**.

Eliminación de una función personalizada

1. Abra el espacio de trabajo Central Administration.
2. Abra la página User Management.
3. Abra la pestaña User Roles and Permissions.
4. Haga clic en **Delete a Role**.
   Se abre el cuadro de diálogo Delete a User Role.

5. Seleccione la función que desea eliminar y, a continuación, haga clic en **OK**.

Grupos de trabajo

Use la página Workgroup Management para gestionar grupos de trabajo. Los grupos de trabajo tienen usuarios, estaciones de trabajo y proyectos.

Cree un grupo de trabajo agregando recursos de los grupos correspondientes. Antes de crear un grupo de trabajo, asegúrese de añadir todos los posibles usuarios al grupo de usuarios, las estaciones de trabajo al conjunto de estaciones de trabajo y los directorios principales de proyecto al conjunto de proyectos.

Si es necesario, añada funciones adicionales. También puede seleccionar el modo de seguridad para cada grupo de trabajo.

Si la estación de trabajo se ha registrado en el software Central Administrator Console (CAC) y es miembro del grupo de trabajo, la configuración del modo de seguridad del grupo de trabajo tendrá prioridad sobre la configuración del modo de seguridad de la estación de trabajo.

No agregue usuarios locales a grupos de trabajo. El software CAC es una aplicación de red, por lo que solo deben agregarse usuarios de red a un grupo de trabajo.

Nota: En cada grupo de trabajo, al menos un usuario debe tener asignada la función de administrador. Si el usuario que haya iniciado sesión no está disponible en ese momento, solo podrá desbloquear la pantalla del software CAC un administrador o un supervisor.

Si la seguridad basada en servidor ya no es necesaria para una estación de trabajo concreta, puede gestionar la seguridad de la estación de trabajo localmente con SCIEX OS.

Crear un grupo de trabajo

1. Abra el espacio de trabajo Central Administration.
2. Abra la página Workgroup Management.
3. Haga clic en **Add Workgroup** ( ).
   Se abre el cuadro de diálogo Add a Workgroup.
4. Escriba un nombre en el campo **Workgroup Name**.
5. Escriba un nombre en el campo **Description** y, seguidamente, haga clic en **Add**.
   El grupo de trabajo se crea y se añade al panel Manage Workgroups and Assignments. El software Central Administrator Console (CAC) crea el nombre de grupo de trabajo adecuado en el servidor.

   Nota: El modo integrado es la configuración de seguridad predeterminada.

Eliminar un grupo de trabajo

Si un grupo de trabajo ya no es necesario, elimínelo de la lista de grupos de trabajo. Al eliminar un grupo de trabajo, solo se elimina del software Central Administrator Console (CAC). No se pierde ningún dato de la estación de trabajo.

1. Abra el espacio de trabajo Central Administration.
2. Abra la página Workgroup Management.
3. Expanda la lista **Workgroups** y busque el grupo de trabajo que desee eliminar. Haga clic en **Delete**.
   Se abre el cuadro de diálogo Delete Workgroup.
4. Haga clic en **Yes**.

Agregar usuarios o grupos a un grupo de trabajo

Nota: A los usuarios añadidos al grupo de trabajo no se les asigna una función automáticamente. Para asignar funciones a los usuarios, consulte la sección: Añadir o eliminar una función.

1. Abra el espacio de trabajo Central Administration.
2. Abra la página Workgroup Management.
3. En el panel Manage Workgroups and Assignments, expanda el grupo de trabajo que se debe cambiar y, a continuación, expanda la lista **Users**.
4. Seleccione un usuario o un grupo y, a continuación, haga clic en **Add** ().

   Sugerencia: Añada o seleccione varios usuarios pulsando la tecla **Shift** a la vez que selecciona los usuarios correspondientes.

   El usuario o grupo se añade al grupo de trabajo actual.
5. Asigne una o más funciones al usuario o grupo añadido. Consulte la sección: Añadir o eliminar una función.
6. Haga clic en **Save**.

Añadir o eliminar una función

Procedimientos de condiciones previas
• Agregar usuarios o grupos a un grupo de trabajo.

Para obtener información sobre la creación de funciones en el software Central Administrator Console (CAC), consulte la sección Añadir una función personalizada. Los usuarios o grupos con una función asignada tienen todos los permisos asociados con la función. Los usuarios o grupos pueden tener más de una función a la vez.

1. Abra el espacio de trabajo Central Administration.

2. Abra la página Workgroup Management.
3. En el panel Manage Workgroups and Assignments, expanda el grupo de trabajo que se debe cambiar y, a continuación, expanda la lista **Users**.
4. En la sección Current Workgroup Membership, asigne o elimine funciones en la columna **Assign Roles**.
5. Haga clic en **Save**.

Añadir estaciones de trabajo a un grupo de trabajo

Nota: Una estación de trabajo solo aparece en el conjunto de estaciones de trabajo si se ha registrado con el software Central Administrator Console (CAC). Consulte la sección Adición de una estación de trabajo

1. Abra el espacio de trabajo Central Administration.
2. Abra la página Workgroup Management.
3. En el panel Manage Workgroups and Assignments, expanda el grupo de trabajo que se debe cambiar y, a continuación, expanda la lista **Workstations**.
4. Seleccione una estación de trabajo y, a continuación, haga clic en **Add** (). La estación de trabajo se añade al grupo de trabajo actual.
5. Haga clic en **Save**.

Asignar configuración de seguridad de grupo de trabajo

Procedimientos de condiciones previas
• Adición de una estación de trabajo • Añadir estaciones de trabajo a un grupo de trabajo

Para obtener información sobre los modos de seguridad, consulte la sección Configuración del modo de seguridad.

1. Abra el espacio de trabajo Central Administration.
2. Abra la página Workgroup Management.
3. En el panel Manage Workgroups and Assignments, expanda el grupo de trabajo que se debe cambiar y, a continuación, expanda la lista **Workstations**.
4. (Opcional) Para que el grupo de trabajo actual sea el grupo de trabajo predeterminado para esa estación de trabajo, seleccione la casilla **Set Default** de la sección Current Workgroup Membership.
5. En la sección Assign Security Settings, seleccione el **Security mode** para el grupo de trabajo y, a continuación, escriba los tiempos correspondientes de **Screen lock** y **Auto logoff**.
6. Haga clic en **Save**.

Añadir proyectos a un grupo de trabajo

Nota: Este procedimiento solo es necesario si el acceso al proyecto se gestiona de forma centralizada.

Nota: Si se añade un proyecto a más de un grupo de trabajo, se añade también el permiso de acceso del usuario, en lugar de sobrescribirse. Por ejemplo, el grupo de trabajo 1 contiene el usuario A, el usuario B y el proyecto_01. El grupo de trabajo 2 contiene el usuario B y el usuario C. Si el proyecto_01 se agrega al grupo de trabajo 2, el usuario A, el usuario B y el usuario C tendrán acceso al proyecto_01.

1. Abra el espacio de trabajo Central Administration.
2. Abra la página Workgroup Management.
3. En el panel Manage Workgroups and Assignments, expanda el grupo de trabajo que se debe cambiar y, a continuación, expanda la lista **Projects**.
4. Seleccione la casilla **Use central settings for projects**.
   Aparece la sección de selección de proyecto.
5. Seleccione un **Project root directory** para añadir un grupo entero de proyectos o expanda el directorio principal y seleccione un proyecto específico para añadirlo al grupo de trabajo.
6. Haga clic en **Add** () para añadir los proyectos al grupo de trabajo.
   El directorio principal del proyecto se añade a la tabla Current Workgroup Membership. Expanda el directorio principal del proyecto para ver los proyectos actuales del grupo de trabajo.
7. Haga clic en **Save**.

Gestionar proyectos

Use la página Project Management para crear, modificar y eliminar proyectos.

Para acceder a un proyecto, los usuarios deben tener acceso al directorio principal en el que se almacenan los datos del proyecto. Para obtener más información, consulte la sección Acerca de los proyectos y directorios principales.

Acerca de los proyectos y directorios principales

Un directorio principal o raíz es una carpeta que contiene uno o varios proyectos. Es la carpeta en la que el software busca los datos del proyecto. El directorio raíz predefinido es `D:\SCIEX OS Data`.

Para asegurarse de que la información del proyecto se almacena de forma segura, cree los proyectos con el software Central Administrator Console (CAC). Añada proyectos al Project Root Pool antes de añadirlos a un grupo de trabajo. Consulte la sección: Adición de un proyecto.

Los datos del proyecto se pueden organizar en subcarpetas. Cree las subcarpetas con el software CAC. Consulte la sección: Adición de una subcarpeta.

Nota: Si un proyecto se crea fuera del software CAC, el directorio principal del proyecto debe actualizarse después de crear el proyecto. Cuando se actualiza el directorio principal, se sincroniza el contenido de Project Root Pool con el contenido de los directorios principales del proyecto en la red.

Adición de un directorio raíz

Un directorio raíz es la carpeta en la que se almacenan uno o varios proyectos.

Nota: El software guarda hasta diez directorios raíz.

Sugerencia: No es posible acceder a las unidades locales desde la red. Un directorio principal solo se puede crear en una unidad compartida.

1. Abra el espacio de trabajo Central Administration.
2. Abra la página Project Management.
3. Haga clic en **Add new or existing project root to project pool** ().
   Se abre el cuadro de diálogo Add Root Directory.
4. Escriba la ruta completa del directorio principal y, a continuación, haga clic en **OK**.
   Se crea la carpeta.

   Sugerencia: En vez de escribir la ruta, haga clic en **Browse** y seleccione la carpeta en la que se creará el directorio.

   Sugerencia: De forma alternativa, cree una carpeta en el Explorador de archivos y, a continuación, busque y seleccione la carpeta.

   Nota: En el caso de instalaciones de SCIEX OS con una licencia de procesamiento, el directorio raíz puede ser una carpeta del software Analyst carpeta (`Analyst Data\Projects`) del software.
5. Haga clic en **OK**.
   El nuevo directorio raíz pasa a ser el directorio raíz del proyecto actual.

Eliminar un directorio principal del proyecto

El software conserva una lista de los diez últimos directorios principales que se han usado. El usuario puede eliminar directorios principales de esta lista.

Nota: Al eliminar un directorio principal, también se eliminan todos los proyectos asociados desde el conjunto de directorios principales del proyecto.

1. Abra el espacio de trabajo Central Administration.

2. Abra la página Project Management.
3. Busque el directorio principal del proyecto que desee eliminar y, a continuación, haga clic en **Delete Project Root** en la sección Actions.
   El software solicita confirmación.
4. Haga clic en **OK**.

Adición de un proyecto

Procedimientos de condiciones previas
• Adición de un directorio raíz

El proyecto almacena métodos de adquisición, datos, lotes, métodos de procesamiento, resultados de procesamiento, etc. Recomendamos el uso de carpetas de proyecto independientes para cada proyecto.

No cree proyectos ni copie ni pegue archivos fuera del software Central Administrator Console (CAC).

1. Abra el espacio de trabajo Central Administration.
2. Abra la página Project Management.
3. Haga clic en **Add project** en la sección Actions del directorio principal.
   Se abre el cuadro de diálogo New Project.
4. Escriba el nombre del proyecto.
5. Haga clic en **OK**.
   El nuevo proyecto se muestra en el directorio principal.

Adición de una subcarpeta

Los datos de los proyectos se pueden organizar también en subcarpetas.

1. Abra el espacio de trabajo Central Administration.
2. Abra la página Project Management.
3. Haga clic en **Add data sub-folders** en la sección Actions del directorio principal.
   Se abre el cuadro de diálogo Add Data Sub-Folders.
4. Seleccione el proyecto al que pertenecerá la subcarpeta.
5. Haga clic en **Add a new data sub-folder** ().
   Se abre el cuadro de diálogo Data Sub-Folder Name.
6. Escriba el nombre de la subcarpeta.
7. Haga clic en **Save**.

Sugerencia: Las subcarpetas se pueden anidar en otras subcarpetas. Para crear una subcarpeta anidada, seleccione una subcarpeta existente en la sección Project Data Sub-Folders y haga clic en **Add a new data sub-folder** ( ).

8. Cierre el cuadro de diálogo Add Data Sub-Folders.

Estaciones de trabajo

Use la página Workstation Management para gestionar todas las estaciones de trabajo conectadas con el servidor de CAC. A las estaciones de trabajo que están bajo el control del software CAC se les aplica automáticamente una configuración personalizada.

Adición de una estación de trabajo

En la página Workstation Management, los administradores pueden añadir o eliminar estaciones de trabajo del control del software Central Administrator Console (CAC).

1. Abra el espacio de trabajo Central Administration.
2. Abra la página Workstation Management.
3. Haga clic en **Add Workstation to the Workstations Pool** ( ).
   Se abre el cuadro de diálogo Select Computers.
4. Escriba los nombres de las estaciones de trabajo que se deben añadir y haga clic en **OK**.

Eliminar una estación de trabajo

Si una estación de trabajo ya no se utiliza o ya no es necesaria en un grupo de trabajo, elimínela del conjunto de estaciones de trabajo. Al eliminar una estación de trabajo, se elimina de todos los grupos de trabajo a los que se hubiera asignado. No se pierde ningún dato de la estación de trabajo al eliminarla.

1. Abra el espacio de trabajo Central Administration.
2. Abra la página Workstation Management.
3. Haga clic en **Workstation Management**.
4. En el panel Workstation Pool, busque la estación de trabajo que desee eliminar y, a continuación, haga clic en **Delete**.
   Se abre el cuadro de diálogo Delete Workstation.
5. Haga clic en **OK**.

Informes y funciones de seguridad

Generar informes de datos de grupos de trabajo

Los usuarios pueden generar informes de datos que incluyan información como usuarios configurados, funciones, estaciones de trabajo, proyectos y grupos de trabajo.

1. Abra el espacio de trabajo Central Administration.
2. Haga clic en **Print**.
   Se abre el cuadro de diálogo Print.
3. Defina las opciones de impresión y, a continuación, haga clic en **Print**.
4. (Solo imprimir a PDF) Busque la ubicación en la que desee guardar el informe y haga clic en **Save**.

Exportar la configuración de software de CAC

El usuario puede exportar la configuración de seguridad que se puede aplicar a otro servidor de Central Administrator Console (CAC). La configuración se exporta como archivo ecac.

1. Abra el espacio de trabajo Central Administration.
2. Haga clic en **Advanced** > **Export CAC settings**.
   Se abre el cuadro de diálogo Export CAC Settings.
3. Haga clic en **Browse**.
4. Busque y seleccione la carpeta donde se guardará la configuración y, a continuación, haga clic en **Select Folder**.
5. Haga clic en **Export**.
   Aparecerá un mensaje de confirmación con el nombre del archivo que contiene la configuración exportada.
6. Haga clic en **OK**.

Importar la configuración de software de CAC

Procedimientos de condiciones previas
• Exportar la configuración de software de CAC

El usuario puede importar la configuración de seguridad de SCIEX OS u otros servidores de Central Administrator Console (CAC). La configuración se importa de un archivo ecac.

1. Abra el espacio de trabajo Central Administration.
2. Haga clic en **Advanced** > **Import CAC settings**.
   Se abre el cuadro de diálogo Import CAC Settings.
3. Haga clic en **Browse**.

4. Busque y seleccione el archivo que contiene la configuración que desea importar y, a continuación, haga clic en **Open**.
   El software se asegura de que el archivo sea válido.
5. Haga clic en **Import**.
   El software realiza una copia de seguridad de la configuración actual e importa la nueva configuración. Se muestra un mensaje de confirmación.

   Nota: La configuración importada se aplica una vez reiniciado el software CAC.
6. Haga clic en **OK**.

Restaurar configuración de software CAC

El usuario puede importar automáticamente la última configuración ecac exportada.

1. Abra el espacio de trabajo Central Administration.
2. Haga clic en **Advanced** > **Restore CAC settings**.
   Se abre el cuadro de diálogo Restore CAC Settings.

   Nota: La configuración restaurada se aplica una vez reiniciado el software Central Administrator Console (CAC).
3. Haga clic en **Yes**.

Adquisición en red 6

En esta sección se describe cómo funciona la adquisición en red en SCIEX OS y las ventajas y limitaciones de los proyectos basados en una red. También contiene procedimientos para configurar la adquisición en red.

Acerca de la adquisición en red

La adquisición en red se puede usar para adquirir datos de uno o más instrumentos en carpetas de proyecto basado en la red que se puedan procesar en estaciones de trabajo remotas. Este proceso tolera fallos de red y asegura que no se pierdan datos si la conexión falla durante la adquisición.

El rendimiento del sistema se puede ralentizar cuando se usan proyectos de red en lugar de proyectos locales. Como algunas pistas de auditoría también residen en las carpetas de red, cualquier actividad que genere un registro de auditoría de proyecto será más lento. Puede que los archivos de red tarden algún tiempo en abrirse, dependiendo del rendimiento de la red. El rendimiento de la red no solo está relacionado con el hardware físico de la red, sino también con el tráfico y el diseño de esta.

Nota: Si durante la adquisición de red se interrumpe el servicio ClearCore2, los datos parciales de la muestra que está en proceso de adquisición en el momento de la interrupción no se escribirán en el archivo de datos.

Nota: Cuando se utiliza la adquisición en red en un entorno regulado, se debe sincronizar la hora del ordenador local con la hora del servidor para que las marcas de hora sean exactas. La hora del servidor es la que se utiliza para la hora de creación del archivo. El gestor de pistas de auditoría registra la hora de creación de archivos según la hora del ordenador local.

PRECAUCIÓN: Posible pérdida de datos. No guarde datos de varios ordenadores de adquisición en el mismo archivo de datos de red.

Ventajas de usar la adquisición en red

La adquisición de datos en red proporciona un método seguro de trabajar con carpetas de proyecto que residan enteramente en servidores de red. Esto reduce la complejidad de la recolección de datos localmente para luego moverlos a una ubicación de red para su almacenamiento. Asimismo, debido a que habitualmente se hacen copias de seguridad automáticas de las unidades de red, se reduce o elimina la necesidad de realizar copias de seguridad de las unidades locales.

Cuenta de red segura

En un entorno regulado en el que se adquieren datos en una carpeta de red, se recomienda encarecidamente que los usuarios no tengan derechos de eliminación para la carpeta de destino. Sin embargo, sin acceso de eliminación a esta carpeta, SCIEX OS no puede funcionar de forma óptima. La característica de cuenta de red segura (SNA) identifica una cuenta de red que tiene el permiso de archivo de control total para el directorio principal de red. El servicio ClearCore2 utiliza esta cuenta para transferir datos a la carpeta de red.

La SNA debe tener control total para:

- La carpeta del directorio principal de la red
- La carpeta `SCIEX OS Data\NetworkBackup` del ordenador de adquisición
- La carpeta `SCIEX OS Data\TempData` del ordenador de adquisición

No es necesario que la SAA:

- Pertenezca al grupo de administradores del ordenador.
- Esté en la base de datos de administración de usuarios del software SCIEX OS.

La SNA se especifica en la página Projects del espacio de trabajo Configuration. Solo se puede especificar una cuenta de red o dominio de Windows válida.

Si no se especifica una SNA, SCIEX OS usa las credenciales del usuario de la cuenta de Windows que haya iniciado sesión para transferir los datos al directorio principal de red. Para que la transferencia se realice adecuadamente, la cuenta debe tener permisos de escritura para todas las carpetas del proyecto para las que se están adquiriendo datos, independientemente del usuario que haya enviado el lote para adquisición.

Proceso de transferencia de datos

Cuando SCIEX OS adquiere datos para una ubicación de red, primero escribe cada muestra en una carpeta en la unidad local y después la transfiere a la red. Cuando se confirma que todo el archivo de datos se ha transferido correctamente, se elimina la carpeta local que contiene los datos. Si la red deja de estar disponible durante este proceso, SCIEX OS lo vuelve a intentar cada 15 minutos hasta que se realiza la transferencia correctamente.

Para obtener información sobre el acceso a los datos durante períodos prolongados de pérdida de conectividad de la red, consulte la sección Eliminación de las muestras de las carpetas de transferencia en red.

Configuración de la adquisición en red

Un directorio raíz es la carpeta en la que SCIEX OS guarda datos. Para asegurarse de que la información del proyecto se almacena de forma segura, cree el directorio raíz mediante SCIEX OS. No cree proyectos en el explorador de archivos.

Opcionalmente, al crear directorios raíz en un recurso de red, defina las **Credentials for Secure Network Account**. Esta es cuenta de red segura definida en el recurso de red. Consulte la sección Cuenta de red segura.

Para obtener información sobre cómo crear proyectos y subproyectos, consulte el documento *Guía de usuario del software de SCIEX OS*.

Especificación de una cuenta de red segura

Si los proyectos se guardan en un recurso de red, se puede especificar una SNA para asegurarse de que todos los usuarios de la estación de trabajo tienen el acceso necesario al recurso de red.

1. Abra el espacio de trabajo Configuration.
2. Haga clic en **Projects**.
3. En la sección **Advanced**, haga clic en **Credentials for Secure Network Account**.
4. Escriba el nombre de usuario, la contraseña y el dominio de la cuenta de red segura definida en el recurso de red.
5. Haga clic en **OK**.

Auditoría 7

En esta sección se explica cómo utilizar la función de auditoría del software. Para obtener información acerca de las funciones de auditoría de Windows, consulte la sección: Auditorías del sistema .

Pistas de auditoría

Los eventos auditados se almacenan en pistas de auditoría. Hay dos tipos de pistas de auditoría disponibles: estación de trabajo y proyecto.

Las pistas de auditoría de estación de trabajo son archivos que almacenan los eventos auditados para el ordenador en el que se ejecuta SCIEX OS o el software Central Administrator Console (CAC). Para ver una lista completa de los eventos auditados, consulte la sección: Pista de auditoría de la estación de trabajo.

Una pista de auditoría de proyecto es el archivo en el que se almacenan los eventos auditados del proyecto. Para ver una lista completa de los eventos auditados, consulte la sección: Pista de auditoría del proyecto. En SCIEX OS y el software CAC, el espacio de trabajo Audit Trail muestra las pistas de auditoría para los proyectos del directorio principal actual. Los eventos de pista de auditoría de proceso están incluidos en el mapa de pista de auditoría del proyecto y se guardan con la tabla de resultados.

Las pistas de auditoría, combinadas con archivos como los archivos wiff2 y de tablas de resultados, conforman registros electrónicos válidos que se pueden utilizar con fines de cumplimiento normativo.

Tabla 7-1: Pistas de auditoría del software

Pista de auditoría	Ejemplos de eventos registrados	Mapas de auditoría disponibles almacenados en	Mapas de auditoría predeterminados

Estación de trabajo (SCIEX OS)	• Cambios en:
	  • Asignación del mapa de auditoría activo
	  • Ajuste del instrumento
	  • Colas de muestras
	  • Seguridad
	  • Ajustes
	  • Dispositivos
		• Carpeta `C:\ProgramData\SCIEX\Audit Data`	• No hay mapa de auditoría

Tabla 7-1: Pistas de auditoría del software (continuación)

Pista de auditoría	Ejemplos de eventos registrados	Mapas de auditoría disponibles almacenados en	Mapas de auditoría predeterminados

Estación de trabajo (CAC)	• Cambios en:
	  • Mapa de auditoría
	  • CAC Server
	  • Seguridad
	  • Registro de usuario
		• Carpeta `C:\ProgramData\SCIEX\Audit Data`	• Mapa de auditoría silencioso

Proyecto (uno por proyecto)	• Cambios en:
	  • Asignación del mapa de auditoría activo (SCIEX OS)
	  • Proyecto
	  • Datos
	• Impresión
		• Carpeta `<project>\Audit Data`	• Se especifica en la página Audit Maps del espacio de trabajo Configuration

Cuando la pista de auditoría de una estación de trabajo o un proyecto contiene 20 000 registros de auditoría, SCIEX OS el software CAC archiva automáticamente los registros y comienza una nueva pista de auditoría. Para obtener más información, consulte la sección Archivos de pistas de auditoría.

Mapas de auditoría

Un mapa de auditoría es un archivo que contiene una lista de los eventos que se pueden auditar y si se necesita un motivo del cambio o una firma electrónica para el evento. Hay dos tipos de mapas de auditoría disponibles: estación de trabajo y proyecto.

Los mapas de auditoría de la estación de trabajo controlan los eventos que se auditan en una estación de trabajo.

Los mapas de auditoría del proyecto controlan los eventos que se auditan en un proyecto y se almacenan en la carpeta de proyecto.

Nota: El mapa de auditoría de un proyecto se puede editar en SCIEX OS o en el software Central Administrator Console (CAC).

El usuario puede crear muchos mapas de auditoría de estación de trabajo y proyecto, pero solo se puede usar uno cada vez para cada estación de trabajo y cada proyecto. El mapa

de auditoría en uso para una estación de trabajo o proyecto se denomina mapa de auditoría activo.

Cuando se instala SCIEX OS, el mapa de auditoría predeterminado para todos los proyectos nuevos es No Audit Map. Cuando se instala el software CAC el mapa de auditoría predeterminado para todos los proyectos nuevos es Silent Audit Map. El usuario puede identificar un mapa de auditoría diferente para usarlo como el predeterminado para todos los proyectos nuevos. Consulte la sección Cambio del mapa de auditoría activo para un proyecto.

Configuración de mapas de auditoría

Antes de comenzar a trabajar con proyectos para los que sea necesario realizar auditorías, debe configurar mapas de auditoría apropiados para los procedimientos de funcionamiento estándar. Hay varias plantillas del mapa de auditoría predeterminadas disponibles cuando se instala el software, pero puede ser necesario crear un mapa personalizado. Debe asegurarse de que haya disponible un mapa de auditoría adecuado para la pista de auditoría de la estación de trabajo y un mapa de auditoría apropiado para cada proyecto.

Tabla 7-2: Lista de comprobación para configurar la auditoría

Tarea	Consulte
Crear un mapa de auditoría para la pista de auditoría de la estación de trabajo.	• Creación de un mapa de auditoría de estación de trabajo. • Edición de un mapa de auditoría de estación de trabajo.
Aplicar el mapa de auditoría a la pista de auditoría de la estación de trabajo.	• Cambio del mapa de auditoría activo para una estación de trabajo.
Crear un mapa de auditoría activo predeterminado para los proyectos nuevos.	• Creación de un mapa de auditoría de proyecto.
Configurar el mapa de auditoría para usarlo en cada proyecto existente.	• Creación de un mapa de auditoría de proyecto. • Edición de un mapa de auditoría de proyecto.
Aplicar un mapa de auditoría a cada proyecto existente.	• Cambio del mapa de auditoría activo para un proyecto.

Plantillas del mapa de auditoría instaladas

El software incluye distintas plantillas del mapa de auditoría. Estas plantillas no se pueden editar ni borrar.

Tabla 7-3: Mapas de auditoría instalados

Mapa de auditoría	Descripción
Mapa de auditoría de ejemplo	Se auditan los eventos seleccionados. Únicamente con fines ilustrativos.
Mapa de auditoría completo	Se auditan todos los eventos. Se requieren firmas electrónicas y motivos para todos los eventos.
No hay mapa de auditoría	No se audita ningún evento. **Nota:** El evento **Change Active Audit Map Assignment** siempre se registra, incluso si no se usa ninguna plantilla de mapa de auditoría.
Mapa de auditoría silencioso	Se auditan todos los eventos. No se requieren firmas electrónicas ni motivos para ningún evento.

Para obtener una descripción de los tipos de pistas de auditoría y su relación con los mapas de auditoría, consulte la Tabla 7-1. Para obtener más información acerca de los eventos registrados en las pistas de auditoría, consulte la sección Registros de pistas de auditoría.

Para obtener información acerca del proceso de auditoría, consulte la tabla: Tabla 7-2.

Trabajo con mapas de auditoría

El software incluye distintas plantillas instaladas del mapa de auditoría. Para obtener una descripción de las plantillas del mapa de auditoría, consulte la sección: Plantillas del mapa de auditoría instaladas. Para obtener una lista de comprobación de los pasos recomendados para configurar las auditorías, consulte la sección: Configuración de mapas de auditoría.

Si se elimina una plantilla de mapa de auditoría activa en el software o en el explorador de archivos, el proyecto que utilice esa plantilla de mapa de auditoría utilizará Silent Audit Map.

Mapas de auditoría de proyecto

Los mapas de auditoría del proyecto controlan la auditoría de los eventos del proyecto. Para ver una lista de los eventos del proyecto auditables, consulte la sección Pista de auditoría del proyecto.

Creación de un mapa de auditoría de proyecto

1. Abra el espacio de trabajo Configuration.
2. Haga clic en **Audit Maps**.
3. Abra la pestaña Projects Templates.

4. En el campo **Edit map template**, seleccione una plantilla para usarla como base para el nuevo mapa.
5. Haga clic en **Add Template** ().
   Se abre el cuadro de diálogo Add a Project Audit Map Template.
6. Escriba el nombre del nuevo mapa y haga clic en **OK**.
7. Seleccione y configure los eventos que se deben registrar siguiendo los siguientes pasos:
   a. Seleccione la casilla **Audited** para el evento.
   b. (Opcional) Si es necesario indicar un motivo, seleccione **Reason Required**.
   c. (Opcional) Si se necesita una firma electrónica, seleccione **E-Sig Required**.
   d. (Opcional) Si se necesitan motivos predefinidos, seleccione **Use Predefined Reason Only** y defina los motivos.
8. Asegúrese de que la casilla **Audited** no esté seleccionada para los eventos que no se van a auditar.
9. Haga clic en **Save Template**.
   El sistema indica al usuario que aplique el nuevo mapa a los proyectos.
10. Realice una de las siguientes acciones:
    - Para aplicar el nuevo mapa a los proyectos, haga clic en **Yes**, seleccione los proyectos que van a usar el nuevo mapa y haga clic en **Apply**.
    - Si el nuevo mapa no se va aplicar a proyectos existentes, haga clic en **No**.
11. (Opcional) Para usar este mapa de auditoría como el predeterminado para todos los proyectos nuevos, haga clic en **Use as Default for New Projects**.

Edición de un mapa de auditoría de proyecto

Nota: No se pueden editar las plantillas del mapa de auditoría instaladas.

1. Abra el espacio de trabajo Configuration.
2. Haga clic en **Audit Maps**.
3. Abra la pestaña Projects Templates.
4. En el campo **Edit map template**, seleccione el mapa que hay que modificar.
5. Seleccione y configure los eventos que se deben registrar siguiendo los siguientes pasos:
   a. Seleccione la casilla **Audited** para el evento.
   b. (Opcional) Si es necesario indicar un motivo, seleccione **Reason Required**.
   c. (Opcional) Si se necesita una firma electrónica, seleccione **E-Sig Required**.

d. (Opcional) Si se necesitan motivos predefinidos, seleccione **Use Predefined Reason Only** y defina los motivos.

6. Asegúrese de que la casilla **Audited** no esté seleccionada para los eventos que no se van a auditar.
7. Haga clic en **Save Template**.
   El sistema indica al usuario que aplique el nuevo mapa a los proyectos.
8. Realice una de las siguientes acciones:
   - Para aplicar el nuevo mapa a los proyectos, haga clic en **Yes**, seleccione los proyectos que van a usar el nuevo mapa y haga clic en **Apply**.
   - Si el nuevo mapa no se va aplicar a proyectos existentes, haga clic en **No**.

Cambio del mapa de auditoría activo para un proyecto

Cuando se aplica un mapa de auditoría al proyecto, este se convierte en el mapa de auditoría activo. La configuración de auditoría del mapa de auditoría activo determina qué eventos se registran en las pistas de auditoría.

1. Abra el espacio de trabajo Configuration.
2. Haga clic en **Audit Maps**.
3. Abra la pestaña Projects Templates.
4. En el campo **Edit map template**, seleccione el mapa de auditoría que se asignará al proyecto.
5. Haga clic en **Apply to Existing Projects**.
   Se abre el cuadro de diálogo Apply Project Audit Map Template.
6. Selecciona las casillas para los proyectos para los que se aplicarán este mapa de auditoría.
7. Haga clic en **Apply**.

Eliminación de un mapa de auditoría de proyecto

Nota: No se pueden eliminar las plantillas del mapa de auditoría instaladas.

1. Abra el espacio de trabajo Configuration.
2. Haga clic en **Audit Maps**.
3. Abra la pestaña Projects Templates.
4. En el campo **Edit map template**, seleccione el mapa que desea eliminar.
5. Haga clic en **Delete Template**.
   El sistema solicita confirmación.
6. Haga clic en **Yes**.

Mapas de auditoría de la estación de trabajo

Los mapas de auditoría de la estación de trabajo controlan la auditoría de los eventos de la estación de trabajo. Para ver una lista de los eventos auditables de la estación de trabajo, consulte la sección Pista de auditoría de la estación de trabajo.

Creación de un mapa de auditoría de estación de trabajo

1. Abra el espacio de trabajo Configuration.
2. Haga clic en **Audit Maps**.
3. Abra la pestaña Workstation Templates.
4. En el campo **Edit map template**, seleccione una plantilla para usarla como base para el nuevo mapa.
5. Haga clic en **Add Template** ( ).
   Se abre el cuadro de diálogo Add a Workstation Audit Map Template.
6. Escriba el nombre del nuevo mapa y haga clic en **OK**.
7. Seleccione y configure los eventos que se deben registrar siguiendo los siguientes pasos:
   a. Seleccione la casilla **Audited** para el evento.
   b. (Opcional) Si es necesario indicar un motivo, seleccione **Reason Required**.
   c. (Opcional) Si se necesita una firma electrónica, seleccione **E-Sig Required**.
   d. (Opcional) Si se necesitan motivos predefinidos, seleccione **Use Predefined Reason Only** y defina los motivos.
8. Asegúrese de que la casilla **Audited** no esté seleccionada para los eventos que no se van a auditar.
9. Haga clic en **Save Template**.
10. (Opcional) Para usar este mapa de auditoría como mapa de auditoría activo para la estación de trabajo, haga clic en **Apply to the Workstation**.

Edición de un mapa de auditoría de estación de trabajo

Nota: No se pueden editar las plantillas del mapa de auditoría instaladas.

1. Abra el espacio de trabajo Configuration.
2. Haga clic en **Audit Maps**.
3. Abra la pestaña Workstation Templates.
4. En el campo **Edit map template**, seleccione el mapa que hay que modificar.
5. Seleccione y configure los eventos que se deben registrar siguiendo los siguientes pasos:

a. Seleccione la casilla **Audited** para el evento.

b. (Opcional) Si es necesario indicar un motivo, seleccione **Reason Required**.

c. (Opcional) Si se necesita una firma electrónica, seleccione **E-Sig Required**.

d. (Opcional) Si se necesitan motivos predefinidos, seleccione **Use Predefined Reason Only** y defina los motivos.

6. Asegúrese de que la casilla **Audited** no esté seleccionada para los eventos que no se van a auditar.
7. Haga clic en **Save Template**.
8. (Opcional) Para usar este mapa de auditoría como mapa activo para la estación de trabajo, haga clic en **Apply to the Workstation**.

Cambio del mapa de auditoría activo para una estación de trabajo

Cuando se aplica un mapa de auditoría a la estación de trabajo, este se convierte en el mapa de auditoría activo. La configuración de auditoría del mapa de auditoría activo determina qué eventos se registran en las pistas de auditoría.

1. Abra el espacio de trabajo Configuration.
2. Haga clic en **Audit Maps**.
3. Abra la pestaña Workstation Templates.
4. En el campo **Edit map template**, seleccione el mapa que se aplicará a la estación de trabajo.
5. Haga clic en **Apply to the Workstation**.

Eliminación de un mapa de auditoría de estación de trabajo

Nota: No se pueden eliminar las plantillas del mapa de auditoría instaladas.

1. Abra el espacio de trabajo Configuration.
2. Haga clic en **Audit Maps**.
3. Abra la pestaña Workstation Templates.
4. En el campo **Edit map template**, seleccione el mapa que desea eliminar.
5. Haga clic en **Delete Template**.
   El sistema solicita confirmación.
6. Haga clic en **Yes**.

Ver, buscar, exportar e imprimir pistas de auditoría

En esta sección se proporciona información sobre cómo ver las pistas de auditoría y las pistas de auditoría archivadas. También se proporcionan instrucciones para exportar, imprimir, buscar y ordenar registros de auditoría en pistas de auditoría.

Visualización de pistas de auditoría

1. Abra el espacio de trabajo Audit Trail.
2. Seleccione la pista de auditoría que desee ver:
   - Para ver la pista de auditoría de la estación de trabajo, haga clic en **Workstation**.
   - Para ver una pista de auditoría del proyecto, seleccione el proyecto.
3. Para ver detalles para un registro de auditoría, seleccione el registro.

Búsqueda o filtrado de registros de auditoría

1. Abra el espacio de trabajo Audit Trail.
2. Seleccione la pista de auditoría que desee buscar.
3. Para buscar un registro de auditoría específico, escriba el texto en el campo **Find in Page**.
   Todas las instancias del texto especificado en la página aparecen resaltadas.
4. Para filtrar registros de pista de auditoría, siga los siguientes pasos:
   a. Haga clic en el icono de filtro (embudo).
      Se abre el cuadro de diálogo Filter Audit Trail.
   b. Escriba el criterio de filtro.
   c. Haga clic en **OK**.

Visualización de pistas de auditoría archivadas

Cuando una pista de auditoría alcanza los 20 000 registros de auditoría, SCIEX OS archiva automáticamente los registros y empieza una nueva pista de auditoría. A los archivos de pistas de auditoría se les asigna un nombre que contiene el tipo de pista de auditoría junto con la fecha y la hora. Por ejemplo, el nombre de archivo de un archivo de pista de auditoría tiene el formato WorkstationAuditTrailData-<nombre de la estación de trabajo>-<AAAA><MMDDHHMMSS>.atds

Este procedimiento también se puede usar para abrir una pista de auditoría para la tabla de resultados.

1. Abra el espacio de trabajo Audit Trail.
2. Haga clic en **Browse**.
3. Examine y seleccione la pista de auditoría archivada que desee abrir y haga clic en **OK**.

Nota: Para abrir la pista de auditoría para una tabla de resultados, seleccione el archivo qsession relacionado.

Impresión de pistas de auditoría

1. Abra el espacio de trabajo Audit Trail.
2. Seleccione la pista de auditoría que desee imprimir.

3. Haga clic en **Print**.
   Se abre el cuadro de diálogo Print.
4. Seleccione la impresora y, a continuación, haga clic en **OK**.

Exportación de registros de pista de auditoría

1. Abra el espacio de trabajo Audit Trail.
2. Seleccione la pista de auditoría que desee exportar.
3. Haga clic en **Export**.
4. Vaya a la ubicación en la que se guardará el archivo exportado, escriba un **File name** y haga clic en **Save**.
   La pista de auditoría se guarda como archivo de valores separados por comas (csv).

Registros de pistas de auditoría

En esta sección se describen los campos en los registros de pista de auditoría.

Los archivos de pistas de auditoría de la estación de trabajo y del proyecto son archivos cifrados.

Nota: Las pistas de auditoría y los archivos de la estación de trabajo se guardan en la carpeta `Program Data\SCIEX\Audit Data`. Las pistas de auditoría del proyecto y los archivos se guardan en la carpeta `Audit Data` correspondiente al proyecto.

Tabla 7-4: Campos de registro de eventos

Campo	Descripción
Marca de hora	Fecha y hora del registro.
Nombre del evento	El módulo que ha generado el evento.
Descripción	Una descripción del evento.
Motivo	Motivo del cambio, tal como lo ha especificado el usuario, si es necesario.
E-Signature	Si se proporciona una firma electrónica.
Nombre completo del usuario	El nombre del usuario.
Usuario	El nombre principal del usuario (UPN).
Categoría	El tipo del evento.

Para obtener una lista de todos los eventos que se registran en la estación de trabajo y en las pistas de auditoría del proyecto, consulte las secciones Pista de auditoría de la estación de trabajo y Pista de auditoría del proyecto.

Archivos de pistas de auditoría

Los registros de auditoría se almacenan en los archivos de pistas de auditoría de la estación de trabajo y del proyecto y pueden crear archivos de gran tamaño difíciles de consultar y gestionar.

Cuando una pista de auditoría alcanza los 20 000 registros, se archiva. Se añade un registro de archivo final a la pista de auditoría y esta se guarda con un nombre que indique el tipo de pista de auditoría, la fecha y la hora. Se crea una nueva pista de auditoría. El primer registro de la nueva pista de auditoría indica que la pista de auditoría se ha archivado y especifica la ruta a la pista de auditoría archivada.

Los archivos de la pista de auditoría de la estación de trabajo se guardan en la carpeta `C:\ProgramData\SCIEX\Audit Data`. Los nombres de archivo tienen el formato WorkstationAuditTrailData-<*workstation name*>-<*YYYY*><*MMDDHHMMSS*>.atds. Por ejemplo, `WorkstationAuditTrailData-SWDSXPT158-20190101130401.atds`.

Los archivos de la pista de auditoría del proyecto se guardan en la carpeta `Audit Data` del proyecto.

Acceso a los datos durante interrupciones de red A

Ver y procesar datos localmente

Si se produce una interrupción temporal de la red durante la adquisición en red, se puede acceder a los datos adquiridos desde la carpeta `NetworkBackup` en el ordenador de adquisición. Para evitar que los datos resulten dañados, recomendamos que los archivos de datos en la carpeta `NetworkBackup` se copien a una nueva ubicación antes de visualizarlos o procesarlos, así como guardar una copia de los archivos en la carpeta `NetworkBackup`.

Cada 15 minutos, SCIEX OS determina si la ubicación de red está disponible. Si lo está, se reanuda la transferencia de datos.

La carpeta `NetworkBackup` se almacena en el directorio principal local, normalmente, `D:\SCIEX OS Data\NetworkBackup`. Los archivos de datos para cada lote se almacenan en una carpeta con un identificador único como el nombre de la carpeta. Las marcas de fecha y hora de las carpetas muestran la fecha y hora de inicio del lote y se pueden usar para determinar qué carpeta contiene los datos de interés.

Eliminación de las muestras de las carpetas de transferencia en red

Si se pierde la conectividad de la red durante un periodo de tiempo prolongado o si se cambia el directorio raíz de red, puede que sea necesario eliminar los archivos de datos de las carpetas de transferencia en red. Recomendamos que esta acción la realice un administrador del sistema con un alto nivel de habilidades técnicas.

1. Abra el espacio de trabajo Queue.
2. Detenga la cola.
3. Cancele todas las muestras que queden en el lote y que contengan las muestras que hay que eliminar.
4. Cierre SCIEX OS.
5. Finalice **Clearcore2.Service.exe**.

   Sugerencia: Realice esta tarea desde el Windows Services Manager.

6. Mueva todos los archivos y carpetas de `OutBox` y `NetworkBackup` que están a la espera de trasferirse al directorio raíz no disponible a otra carpeta temporalmente. No elimine las carpetas `OutBox` o `NetworkBackup`.

Nota: `OutBox` es una carpeta oculta en el directorio raíz local, normalmente `D:\SCIEX OS Data\TempData\Outbox`. Cuando ya no se necesiten los archivos y carpetas de `Outbox`, se pueden eliminar.

PRECAUCIÓN: Posible pérdida de datos. No elimine el archivo si deben conservarse los datos de la muestra atascada.

7. Inicie SCIEX OS.
   En 15 minutos, SCIEX OS intenta conectarse al recurso de red. Si la conexión se realiza correctamente, se reanuda la transferencia. Cuando finaliza la transferencia, se eliminan las carpetas de la carpeta `NetworkBackup`.

Eventos de auditoría B

En esta sección se enumeran los eventos de auditoría de SCIEX OS. También se enumeran los eventos de auditoría correspondientes del software Analyst, para los usuarios que están migrando del software Analyst a SCIEX OS.

Pista de auditoría del proyecto

Cada proyecto dispone de una pista de auditoría del proyecto. La pista de auditoría de proyecto se guarda en la carpeta `Audit Data` del proyecto. El nombre de archivo de la pista de auditoría es `ProjectAuditEvents.atds`.

Nota: El mapa de auditoría predeterminado para los nuevos proyectos creados en el software Central Administrator Console (CAC) es el **Silent Audit Map**.

Los eventos de pista de auditoría del proyecto se muestran en el software CAC y en SCIEX OS.

Tabla B-1: Eventos de pista de auditoría del proyecto

SCIEX OS o CAC	Software Analyst
Espacio de trabajo Analytics	
Actual Concentration changed	Eventos de cuantificación: Modificación del valor del campo "Concentration"
Auto-Processing File saved	—
Barcode ID changed	—
Comparison sample changed in non-targeted workflow	—
Custom columns modified	Eventos de cuantificación: Modificación del título en "Custom Title"
Data exploration opened	Eventos del proyecto: Apertura de un archivo de datos
Data exported	—
Data transferred to LIMS	—
Dilution Factor changed	Eventos de cuantificación: Modificación del valor del campo "Dilution Factor"
External calibration changed	—
External calibration exported	—

Tabla B-1: Eventos de pista de auditoría del proyecto (continuación)

SCIEX OS o CAC	Software Analyst
File saved	Eventos del proyecto: Creación de una tabla de resultados de cuantificación, Modificación de una tabla de resultados de cuantificación, Eventos de cuantificación: Se ha guardado una tabla de resultados
Formula column changed	Eventos de cuantificación: Modificación del nombre de la fórmula, Adición del nombre de la fórmula, Modificación de la cadena de la fórmula, Eliminación de la columna de la fórmula
Integration cleared	—
Integration parameters changed	Eventos de cuantificación: Integración del pico de cuantificación
Library search result changed	—
Manual Integration	Eventos de cuantificación: Integración del pico de cuantificación
Manual Integration reverted	Eventos de cuantificación: Restablecimiento del pico de cuantificación original
MS/MS selection changed	—
Processing method changed and applied	Eventos de cuantificación: Modificación del método de cuantificación
Report created	Eventos del proyecto: Impresión en curso de un documento en la impresora, Impresión finalizada de un documento en la impresora
Results Table approved	Eventos de cuantificación: Acceso del revisor de control de calidad a la tabla de resultados
Results Table created	Eventos de cuantificación: Creación de una tabla de resultados
Results Table locked	—
Results Table unlocked	—
Sample ID changed	Eventos de cuantificación: Modificación del valor del campo "Sample ID"
Sample Name changed	Eventos de cuantificación: Modificación del valor del campo "Sample Name"

Tabla B-1: Eventos de pista de auditoría del proyecto (continuación)

SCIEX OS o CAC	Software Analyst
Samples added or removed	Eventos de cuantificación: Adición de archivos a la tabla de resultados, Eliminación de archivos de la tabla de resultados, Adición/eliminación de muestras
Sample Type changed	Eventos de cuantificación: Modificación del valor del campo "Sample Type"
Std. Addition Actual concentration changed	—
Used column selection changed	Eventos de cuantificación: Modificación del valor del campo "Use IT"
Window/pane printed	Eventos del proyecto: Impresión en curso de un documento en la impresora, Impresión finalizada de un documento en la impresora
Página Audit Map	
Project Audit Map changed	Eventos del proyecto: Modificación de la configuración del proyecto
Project Audit Trail Printed	—
Project Audit Trail Exported	—
Espacio de trabajo Batch	
Batch information imported from LIMS/ text	—
Print	Eventos del proyecto: Impresión en curso de un documento en la impresora, Impresión finalizada de un documento en la impresora
Espacio de trabajo Explorer	
Open Sample(s)	Eventos del proyecto: Apertura de un archivo de datos
Recalibrate sample(s)	—
Recalibrate sample(s) started	—
Espacio de trabajo LC Method	
Print	Eventos del proyecto: Impresión en curso de un documento en la impresora, Impresión finalizada de un documento en la impresora
Espacio de trabajo MS Method	

Tabla B-1: Eventos de pista de auditoría del proyecto (continuación)

SCIEX OS o CAC	Software Analyst
Print	Eventos del proyecto: Impresión en curso de un documento en la impresora, Impresión finalizada de un documento en la impresora
Espacio de trabajo Queue	
Sample Transferred	—

Pista de auditoría de la estación de trabajo

Cada estación de trabajo tiene una pista de auditoría de la estación de trabajo. La pista de auditoría de la estación de trabajo se almacena en la carpeta `Program Data\SCIEX\Audit Data`. El nombre de archivo de pista de auditoría está en formato: `WorkstationAuditTrailData.atds`.

Nota: El mapa de auditoría predeterminado para las nuevas estaciones de trabajo creadas en el software Central Administrator Console (CAC) es el **Silent Audit Map**.

Los eventos de pista de auditoría de la estación de trabajo se muestran en el software CAC y en SCIEX OS.

Tabla B-2: Eventos de pista de auditoría de la estación de trabajo

SCIEX OS o CAC	Software Analyst
Instrument Tune (SCIEX OS)	
Firmware changed	—
Manual Tuning	Eventos del instrumento: Modificación de la configuración de ajustes
Automatic Tuning	Eventos del instrumento: Modificación de la configuración de ajustes
Print Procedure Result in MS Tune	Eventos del proyecto: Impresión en curso de un documento en la impresora, Impresión finalizada de un documento en la impresora
Hardware Configuration (SCIEX OS)	
Devices Activated	Eventos del instrumento: Activación del perfil de hardware
Devices Deactivated	Eventos del instrumento: Desactivación del perfil de hardware
Data File Checksum (SCIEX OS)	
Wiff data file checksum has been changed	—

Tabla B-2: Eventos de pista de auditoría de la estación de trabajo (continuación)

SCIEX OS o CAC	Software Analyst
Espacio de trabajo Explorer (SCIEX OS)	
Open Sample(s)	Eventos del proyecto: Apertura de un archivo de datos
Recalibrate samples(s)	—
Recalibrate samples(s) started	—
Página Audit Map[1]	
Workstation Audit Map changed	Eventos del instrumento: Modificación de la configuración del instrumento
Workstation Audit Trail printed	—
Workstation Audit Trail exported	—
CAC Server (CAC)	
Project settings enabled/disabled in a workgroup	—
Project assigned/unassigned to a workgroup	—
User Role(s) assigned/unassigned to user(s) in workgroup	—
User(s)/UserGroup(s) assigned/ unassigned to a workgroup	—
Workgroup added/deleted	—
Workgroup renamed	—
Workstation(s) assigned/unassigned to a workgroup	—
Espacio de trabajo Queue (SCIEX OS)	
Sample moved in Queue	Eventos del instrumento: Desplazamiento de la muestra de la posición X a la posición Y del archivo de lotes
Batch moved in Queue	Eventos del instrumento: Desplazamiento del lote
Reaquiring sample	Eventos del instrumento: Readquisición de muestras
Sample starts to acquire	—

[1] Estos eventos se registran en SCIEX OS y en la CAC.

Tabla B-2: Eventos de pista de auditoría de la estación de trabajo (continuación)

SCIEX OS o CAC	Software Analyst
Print Queue	Eventos del proyecto: Impresión en curso de un documento en la impresora, Impresión finalizada de un documento en la impresora
Sample acquistion has completed	Eventos del proyecto: Adición de una muestra a un archivo de datos
Automatic reinjections Occurred	—
Automatic injection Occurred	—
Seguridad[1]	
Auto logoff by system	Eventos del instrumento: Cierre de sesión de usuario
Forced logoff by another user	Eventos del instrumento: Cierre de sesión de usuario
Forced Logoff failed	—
Screen unlock failed	—
Secure Network Account credentials have been changed	Eventos del instrumento: Modificación de la cuenta de adquisición
Secure Network Account credentials have been removed	Eventos del instrumento: Modificación de la cuenta de adquisición
Secure Network Account credentials have been specified	Eventos del instrumento: Modificación de la cuenta de adquisición
Security configuration changed	Eventos del instrumento: Modificación de la configuración de seguridad, Modificación del bloqueo de la pantalla, Modificación del cierre de sesión
User added/deleted	Eventos del instrumento: Adición de un usuario, Eliminación de un usuario
User has logged in	Eventos del instrumento: Inicio de sesión de usuario
User has logged out	Eventos del instrumento: Cierre de sesión de usuario
User has turned off exclusive mode	—
User Login Failed	Eventos del instrumento: Error de inicio de sesión de usuario
User management settings have been exported	—

Tabla B-2: Eventos de pista de auditoría de la estación de trabajo (continuación)

SCIEX OS o CAC	Software Analyst
User management settings have been imported	—
User management settings have been restored	—
User role assigned to user/user group	Eventos del instrumento: Modificación del tipo de usuario realizada por el usuario
User role deleted	Eventos del instrumento: Eliminación de un tipo de usuario
User role modified	Eventos del instrumento: Modificación del tipo de usuario
UserLog[1]	
Print Event Log	—

Correlación de permisos entre el software SCIEX OS y Analyst C

Esta sección se proporciona para los usuarios que están migrando del software Analyst a SCIEX OS, para ayudarlos a migrar su configuración de seguridad de usuario. Muestra los permisos del software Analyst que corresponden a los permisos de SCIEX OS.

Tabla C-1: Correlación de permisos

SCIEX OS	Software Analyst
Espacio de trabajo Batch	
Submit unlocked methods	—
Open	Batch: Open Existing Batches
Save as	Batch: Create New Batches, Import, Edit Batches, Save Batches, Overwrite Batches
Submit	Batch: Submit Batches
Save	Batch: Save Batches, Overwrite Batches
Save ion reference table	—
Add data sub-folders	—
Configure Decision Rules	—
Espacio de trabajo Configuration	
General tab	—
General: change regional setting	—
General: full screen mode	—
General: Stop Windows services	—
LIMS Communication tab	—
Audit maps tab	Audit Trail Manager: Change Audit Trail Settings, Create or Modify Audit Maps
Queue tab	—
Queue: instrument idle time	—
Queue: max. number of acquired samples	—
Queue: other queue settings	—
Projects tab	—
Projects: create project	Analyst Application: Create Project

Tabla C-1: Correlación de permisos (continuación)

SCIEX OS	Software Analyst
Projects: apply an audit map template to an existing project	Audit Trail Manager: Change Audit Trail Settings
Projects: create root directory	Analyst Application: Create Root Directory
Project: set current root directory	Analyst Application: Set Root Directory
Projects: specify network credentials	—
Projects: Enable checksum writing for wiff data creation	—
Projects: clear root directory	—
Devices tab	Hardware Configuration: Create, Delete, Edit, Activate/Deactivate
User management tab	Configuración de seguridad
Force user logoff	Unlock/Logout Application
Espacio de trabajo Event Log	
Access event log workspace	—
Archive log	—
Espacio de trabajo Audit Trail	
Access audit trail workspace	Audit Trail Manager: View Audit Trail Data
View active audit map	Audit Trail Manager: View Audit Trail Data
Print/Export audit trail	Audit Trail Manager: View Audit Trail Data
Panel Data Acquisition	
Start	—
Stop	—
Save	—
Espacio de trabajo MS Method y LC Method	
Access method workspace	—
New	Acquisition Method: Create/Save acquisition method
Open	Acquisition Method:Open acquisition method as read-only (acquire mode)
Save	Acquisition Method: Overwrite acquisition methods, Create/Save acquisition method

Tabla C-1: Correlación de permisos (continuación)

SCIEX OS	Software Analyst
Save as	Acquisition Method: Overwrite acquisition methods, Create/Save acquisition method
Lock/Unlock method	—
Espacio de trabajo Queue	
Manage	Sample Queue: Reacquire, Delete Sample or Batch, Move Batch
Start/Stop	Sample Queue: Start Sample, Stop Sample, Abort Sample, Stop Queue
Print	Report Template Editor: Print
Espacio de trabajo Library	
Access library workspace	Explore: Setup library location, Setup library user options, Add library record, Add spectrum to library, Modify library record (overrides add/delete if disabled), Delete MS spectrum, Delete UV spectrum, Delete structure, View library, Search library
CAC settings	
Enable Central Administration	—
Espacio de trabajo MS Tune	
Access MS Tune workspace	—
Advanced MS tuning	Tune: Instrument Optimization, Manual Tune, Edit Tuning Options
Advanced troubleshooting	—
Quick status check	Tune: Instrument Opt
Restore instrument data	Tune: Edit Tuning Options, Edit instrument data
Espacio de trabajo Explorer	
Access explorer workspace	—
Export	Explore: Save data to text file
Print	Report Template Editor: Print
Options	—
Recalibrate	Tune: Calibrate from current spectrum
Espacio de trabajo Analytics	

Tabla C-1: Correlación de permisos (continuación)

SCIEX OS	Software Analyst
New results	Quantitation: Create new results tables
Create processing method	Quantitation: Create quantitation methods
Modify processing method	Quantitation: Modify existing methods
Allow Export and Create Report of unlocked Results Table	—
Save results for Automation Batch	—
Change default quantitation method integration algorithm	Quantitation: Change default method options
Change default quantitation method integration parameters	Quantitation: Change default method options
Enable project modified peak warning	—
Add samples	Quantitation: Add and Remove samples from results table
Remove selected samples	Quantitation: Add and Remove samples from results table
Export, import or remove external calibration	—
Modify sample name	Quantitation: Modify sample name
Modify sample type	Quantitation: Modify Sample Type
Modify sample ID	Quantitation: Modify Sample ID
Modify actual concentration	Quantitation: Modify Analyte Concentration
Modify dilution factor	Quantitation: Modify Dilution Factor
Modify comments fields	Quantitation: Modify Sample Comment
Enable manual integration	Quantitation: Manually integrate
Set peak to not found	—
Include or exclude a peak from the results table	Quantitation: Exclude standards from calibration
Regression options	Quantitation: Change regression parameters
Modify the results table integration parameters for a single chromatogram	Quantitation: Change "simple" parameters in peak review, Change "advanced" parameters in peak review
Modify quantitation method for results table component	Quantitation: Edit results tables' method

Tabla C-1: Correlación de permisos (continuación)

SCIEX OS	Software Analyst
Create metric plot new settings	Quantitation: Modify or create metric plot settings
Add custom columns	Quantitation: Create or modify formula columns
Set peak review title format	—
Remove custom column	Quantitation: Create or modify formula columns
Results table display settings	Quantitation: Change results table column precision, Change results table column visibility, Modify results table settings
Lock results table	—
Unlock results table	—
Mark results file as reviewed and save	—
Modify report template	Report Template Editor: Create/Modify report templates
Transfer results to LIMS	—
Modify barcode column	—
Change comparison sample assignment	—
Add the MSMS spectra to library	Explore: Add spectrum to library record
Project default settings	Quantitation: Modify global (default) settings
Create report in all formats	—
Edit flagging criteria parameters	—
Automatic outlier removal parameter change	—
Enable automatic outlier removal	—
Update processing method via FF/LS	—
Update results via FF/LS	—
Enable grouping by adducts functionality	Quantitation: Create Analyte Groups, Modify Analyte Groups
Browse for files	—
Enable standard addition	—

Tabla C-1: Correlación de permisos (continuación)

SCIEX OS	Software Analyst
Set Manual Integration Percentage Rule	Quantitation: Enable or Disable percent rule in Manual Integration

Suma de comprobación de archivos de datos D

Recomendamos que el usuario utilice las sumas de comprobación de archivos de datos para los archivos wiff. La función de suma de comprobación es una comprobación de redundancia cíclica para verificar la integridad del archivo de datos.

Si la función de suma de comprobación de archivos de datos está activada, siempre que el usuario crea un archivo de datos (wiff), el software genera un valor de suma de comprobación utilizando un algoritmo basado en el algoritmo de cifrado público MD5 y guarda el valor en el archivo. Al verificar la suma de comprobación, el software calcula dicha suma y compara este cálculo con la suma de comprobación almacenada en el archivo.

La comparación de las sumas de comprobación puede tener tres resultados:

- Si los valores coinciden, significa que la suma de comprobación es válida.
- Si los valores no coinciden, significa que la suma de comprobación no es válida. Una suma de comprobación no válida indica que el archivo se ha modificado fuera del software o que se ha guardado con la función de cálculo de la suma de comprobación habilitada y esta suma difiere de la suma de comprobación original.
- Si el archivo no contiene un valor de suma de comprobación, no será posible encontrarla. Cuando un archivo no contiene un valor de suma de comprobación almacenado, se debe a que el archivo se ha guardado con la función de suma de comprobación de archivos de datos deshabilitada.

Nota: El usuario puede verificar la suma de comprobación utilizando el software Analyst. Consulte la documentación del software Analyst.

Cómo habilitar o deshabilitar la función de suma de comprobación de archivos de datos

1. Abra el espacio de trabajo Configuration.
2. Haga clic en **Projects**.
3. Si es necesario, expanda **Data File Security**.
4. Para activar la función de suma de comprobación de archivos de datos, seleccione la casilla de verificación **Enable checksum writing for wiff data creation**. Para desactivar la función, desmarque esa casilla de verificación.

Contacto

Formación del cliente

- En América del Norte: NA.CustomerTraining@sciex.com
- En Europa: Europe.CustomerTraining@sciex.com
- Fuera de la UE y América del Norte, visite sciex.com/education para obtener información de contacto.

Centro de aprendizaje en línea

- SCIEX Now Learning Hub

Soporte SCIEX

SCIEX y sus representantes cuentan con un equipo de especialistas técnicos y de servicio totalmente cualificados en todo el mundo. Ellos sabrán resolver sus dudas y preguntas sobre el sistema y cualquier problema técnico que pueda surgir. Para obtener más información, visite el sitio web de SCIEX en sciex.com o póngase en contacto con nosotros de una de las siguientes formas:

- sciex.com/contact-us
- sciex.com/request-support

Ciberseguridad

Para obtener las indicaciones sobre ciberseguridad más recientes para los productos SCIEX, visite sciex.com/productsecurity.

Documentación

Esta versión del documento sustituye a todas las versiones anteriores de este documento.

Para ver este documento electrónicamente se necesita Adobe Acrobat Reader. Para descargar la última versión, vaya a https://get.adobe.com/reader.

Para buscar la documentación relacionada con el producto de software, consulte las notas de la versión o la guía de instalación del software que se suministra con el software.

Para acceder a la documentación del producto de hardware, consulte el DVD de documentación del sistema o el componente.

Las últimas versiones del documento están disponibles en el sitio web de SCIEX, en sciex.com/customer-documents.

Nota: Para solicitar una versión impresa y gratuita de este documento, póngase en contacto con sciex.com/contact-us.