SCIEX
The Power of Precision

Software SCIEX OS

Guia do diretor do laboratório

RUO-IDV-05-7370-PT-L

Agosto de 2023

Este documento é fornecido aos clientes que compraram um equipamento SCIEX para uso na operação de tal equipamento. Este documento é protegido por direitos autorais e qualquer reprodução deste documento ou de qualquer parte do mesmo é estritamente proibida, exceto quando houver autorização por escrito da SCIEX.

O software que pode ser descrito neste documento é fornecido sob um contrato de licença. É contra a lei copiar, modificar ou distribuir o software em qualquer meio de comunicação, exceto se permitido especificamente no contrato de licença. Além disso, o contrato de licença pode proibir que o software seja desmontado, passe por engenharia reversa ou descompilado para qualquer finalidade. As garantias são conforme definidas em tal documento.

Partes deste documento podem fazer referência a outros fabricantes e/ou a seus produtos, podendo conter peças cujos nomes estejam registrados como marcas registradas e/ou funcionem como marcas registradas dos seus respectivos proprietários. Qualquer uso é destinado apenas para designar estes produtos do fabricante como fornecidos pela SCIEX para incorporação em seu equipamento e não implica em qualquer direito e/ou licença para usar ou permitir que outros usem tais nomes de produto, seus e/ou do fabricante como marcas registradas.

As garantias da SCIEX estão limitadas a estas garantias expressas fornecidas no momento da venda ou da licença de seus produtos e são representações, garantias e obrigações únicas e exclusivas da SCIEX. A Sciex não oferece nenhuma outra garantia de nenhum tipo, expressa ou implícita, incluindo, entre outras, garantias de comercialização ou adequação para um propósito particular, decorrentes de um estatuto ou da lei, ou de uma negociação ou utilização comercial expressamente divulgada, e não assume nenhuma responsabilidade ou obrigação contingente, incluindo danos indiretos ou consequentes, para qualquer uso pelo comprador ou por quaisquer circunstâncias adversas decorrentes.

Produto destinado apenas para pesquisa científica. Não destinado ao uso em procedimentos diagnósticos.

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

Índice

Introdução 1

As informações deste manual têm o objetivo de atender dois públicos:

- O administrador do laboratório, que está preocupado com a operação diária e o uso do software SCIEX OS e a instrumentação anexada a partir de uma perspectiva funcional.
- O administrador do sistema, preocupado com a segurança do sistema e a integridade dos dados e do sistema.

Visão geral de configuração de segurança 2

Esta seção descreve como o controle de acesso e os componentes de auditoria do software SCIEX OS funcionam em conjunto com o controle de acesso e os componentes de auditoria do Windows. Descreve também como configurar a Segurança do Windows antes de instalar o software SCIEX OS.

Conformidade regulatória e de segurança

O software SCIEX OS fornece:

- Administração personalizada para atender as necessidades dos requerimentos regulatórios e de pesquisa.
- Ferramentas de segurança e auditoria para suportar conformidade com 21 CFR Part 11 para uso de registro eletrônico.
- Gerenciamento flexível e efetivo de acesso a funções críticas de espectrômetro de massas.
- Acesso controlado e auditado a dados e relatórios vitais.
- Gerenciamento simples de segurança conectado à segurança do Windows.

Requisitos de segurança

Os requisitos de segurança variam de ambientes relativamente abertos, como laboratórios acadêmicos ou de pesquisa, aos mais rigorosamente regulados, como laboratórios de criminalística.

Software SCIEX OS e Segurança do Windows: trabalhando juntos

O software SCIEX OS e o Sistema de arquivos com nova tecnologia (NTFS) do Windows possuem recursos de segurança criados para controlar o sistema e o acesso aos dados.

A segurança do Windows oferece o primeiro nível de proteção ao exigir que os usuários façam login na rede usando uma identificação e senha. Como resultado, somente usuários que são reconhecidos pelo Windows Local ou pelas configurações de segurança da Rede possuem acesso ao sistema. Para obter mais informações, consulte a seção: Configuração da Segurança do Windows.

O SCIEX OS apresenta os seguintes modos de acesso seguro ao sistema:

- Modo misto
- Modo integrado (padrão)

Para obter mais informações sobre os modos de segurança e configurações de segurança, consulte a seção: Configurar o Security Mode.

O SCIEX OS também oferece funções inteiramente configuráveis, separadas dos grupos de usuários associados ao Windows. Ao usar funções, o diretor do laboratório pode controlar o acesso ao software e ao espectrômetro de massas com base em cada função. Para obter mais informações, consulte a seção: Configurar acesso ao software SCIEX OS.

Rastreamentos de auditoria no SCIEX OS e Windows

Os recursos de auditoria do software SCIEX OS, juntamente com os componentes de auditoria integrados do Windows, são essenciais para a criação e o gerenciamento de registros eletrônicos.

SCIEX OS oferece um sistema de rastreamentos de auditorias para atender os requisitos de manutenção de registros eletrônicos. Rastreamentos de auditoria separados registram:

- Alterações às tabelas de resolução ou de calibração de massa, alterações nas configurações do sistema e eventos de segurança.
- Eventos de criação e modificação para projetos, ajuste, lotes, dados, métodos de processamento e arquivos de modelo de relatório, bem como abertura, fechamento de módulos e eventos de impressão. Eventos de exclusão registrados nos rastreamentos de auditoria incluem a exclusão de funções e a exclusão de usuários do software SCIEX OS.
- Criação e modificação das informações da amostra, parâmetros de integração de pico e método de processamento incorporado em uma Tabela de resultados.

Para obter uma lista completa de eventos de auditoria, consulte a seção: Eventos de auditoria.

O software SCIEX OS usa o registro de evento do aplicativo para capturar informações sobre operação de software. Use este registro como auxílio para resolução de problemas. Contém informações detalhadas sobre interações ente espectrômetro de massas, dispositivo e software.

O Windows mantém registros de eventos que capturam uma série de eventos relacionados a segurança, sistema e aplicativo. Na maioria dos casos, a auditoria do Windows é projetada para capturar eventos excepcionais, como registros de falhas. O administrador pode configurar este sistema para configurar uma grande quantidade de eventos, como acesso a arquivos específicos ou atividades administrativas do Windows. Para obter mais informações, consulte a seção: Auditorias do sistema.

Orientação de segurança do cliente: backups

O backup dos dados do cliente é de responsabilidade do cliente. Embora o serviço da SCIEX e o pessoal de suporte possa fornecer aconselhamento e recomendações sobre o backup de dados do cliente, cabe ao cliente se certificar de que o backup dos dados é realizado de acordo com as políticas, as necessidades e os requisitos regulatórios do cliente. A frequência e a cobertura do backup de dados do cliente deve ser proporcional com os requisitos organizacionais e a gravidade dos dados gerados.

Os clientes devem se certificar de que os backups são funcionais, pois backups são um componente vital do gerenciamento geral de dados e essenciais para recuperação caso ocorra ataque malicioso, falha de hardware ou falha de software. Não faça backup do computador durante a aquisição de dados ou se certifique de que os arquivos que estão sendo adquiridos são ignorados pelo software de backup. Recomendamos fortemente que um backup completo seja realizado no computador antes que qualquer atualização de segurança seja instalada ou que qualquer reparo do computador seja realizado. Isso facilitará uma reversão no raro caso de que uma correção de segurança afete qualquer funcionalidade do aplicativo.

21 CFR Part 11

O software SCIEX OS contém os controles técnicos para atender à norma 21 CFR Part 11 com a implementação de:

- Segurança de modo misto e integrado conectada à segurança do Windows.
- Acesso controlado a funcionalidade por meio de funções personalizáveis.
- Rastreamentos de auditoria para operação de instrumentos, aquisição de dados, revisão de dados e geração de relatórios.
- Assinaturas eletrônicas que usam uma combinação de ID de usuário e senha.
- Configuração adequada do sistema operacional Windows.
- Procedimentos e treinamento adequados na empresa.

O software SCIEX OS foi projetado para ser usado como parte de um sistema em conformidade com a 21 CFR Part 11 e pode ser configurado para atender essa norma. O uso do software SCIEX OS em conformidade com a 21 CFR Part 11 depende do uso da licença do SCIEX OS CFR opcional e da configuração do software SCIEX OS. As políticas e os procedimentos necessários, além dos requisitos de treinamentos relacionados, também precisam estar implementados no laboratório.

Os serviços de validação estão disponíveis por meio de Serviços Profissionais SCIEX. Para mais informações, contate complianceservices@sciex.com.

Nota: Não deixe o software Instrument Settings Converter em um sistema validado. Destina-se à transferência inicial das configurações do instrumento do Analyst para o software SCIEX OS. Certifique-se de remover o software Instrument Settings Converter do computador após usá-lo.

Configuração do sistema

A configuração do sistema é geralmente feita pelos administradores de rede ou pessoas com direitos de rede e administração local.

Configuração da Segurança do Windows

Esta seção fornece orientações para a configuração do Windows:

- Siga estas orientações para as contas e senha do Windows:

- A senha do Windows deve ser alterada a cada 90 dias.
- A senha do Windows não pode ser reutilizada por pelo menos uma iteração seguinte. Ou seja, não pode ser a mesma senha anterior.
- A senha do Windows deve possuir no mínimo oito caracteres.
- A senha do Windows deve conter pelo menos dois dos quatro requisitos a seguir para atender aos requisitos de complexidade:
  - Uma letra maiúscula
  - Uma letra minúscula
  - Um valor numérico
  - Um caractere especial (como: ! @ # $ % ^ &)
- O nome de usuário do Windows não pode ser **admin**, **Administrador** ou **demo**.

- Certifique-se de que o administrador do software SCIEX OS possa alterar as permissões dos arquivos da pasta `SCIEX OS Data`. Se essa pasta estiver em um computador local, sugerimos que o administrador do software faça parte do grupo de administradores locais.
- Para garantir que todos os usuários tenham o acesso necessário aos recursos da aquisição de rede, o administrador da rede precisa adicionar uma conta de rede segura (SNA) ao recurso de rede. Essa conta deve possuir permissões de gravação para a pasta da rede que contém o diretório raiz. Ela é definida como SNA nas propriedades do diretório raiz.

Nota: É recomendável que os arquivos da biblioteca sejam importados de uma unidade local.

Nota: Para obter informações sobre as permissões do Windows necessárias para as diferentes funções de usuário, consulte a seção: Permissões do Windows.

Usuários e grupos

O software SCIEX OS usa os nomes e senhas dos usuários registrados no banco de dados de segurança do controlador de domínio principal ou no Active Directory. As senhas são gerenciadas usando as ferramentas oferecidas com o Windows. Para obter mais informações sobre como adicionar e configurar pessoas e funções, consulte a seção: Configurar acesso ao software SCIEX OS.

Suporte do diretório ativo

Ao adicionar usuários ao espaço de trabalho Configuração do SCIEX OS, especifique as contas de usuário em formato UPN (user principal name). As seguintes versões do Active Directory são suportadas:

- Servidores Windows 2012.
- Clientes Windows 7, 64 bits

- Clientes Windows 10, 64 bits

Sistema de arquivos Windows

No software SCIEX OS, os arquivos e diretórios devem ser armazenados em uma partição do disco rígido que use o formato NTFS, que possa controlar e auditar o acesso aos arquivos do software SCIEX OS. O sistema de arquivos FAT (File Allocation Table) não pode controlar nem auditar o acesso a pastas ou arquivos e, portanto, não é adequado para um ambiente seguro.

Permissões de arquivo e pasta

Para administrar a segurança, o administrador do software SCIEX OS precisa ter o direito de alterar as permissões da pasta `SCIEX OS Data`. O acesso deve ser configurado pelo administrador da rede.

Nota: Considere o nível de acesso que os usuários precisam para a unidade, diretório raiz e pastas do projeto em cada computador.Configure compartilhamento e permissões associadas. Para obter mais informações sobre o compartilhamento de arquivos, consulte a documentação do Windows.

Nota: Para evitar problemas com permissões, recomendamos que os arquivos da biblioteca sejam importados de uma unidade local.

Nota: Para obter informações sobre as permissões do Windows necessárias para as diferentes funções de usuário, consulte a seção: Permissões do Windows.

Para obter informações sobre permissões de arquivos e pastas no software SCIEX OS, consulte a seção: Configuração de segurança do software Controle de acesso.

Auditorias do sistema

O recurso de auditoria do sistema Windows pode ser habilitado para detectar brechas de segurança ou invasões ao sistema. A auditoria pode ser configurada para registrar diferentes tipos de eventos relacionados ao sistema. Por exemplo, o recurso de auditoria pode ser habilitado para registrar tentativas de fazer login no sistema no registro de eventos.

Logs de eventos

O Visualizador de Eventos do Windows registra os eventos auditados no registro de segurança, registro do sistema ou registro do aplicativo.

Personalize o registro de eventos da seguinte maneira:

- Configure um tamanho de registro de evento apropriado.
- Habilite a substituição automática de eventos antigos.
- Defina as configurações de segurança do computador Windows.

Um processo de revisão e armazenamento pode ser implementado. Para obter mais informações sobre configurações de segurança e políticas de auditoria, consulte a documentação do Windows.

Alertas do Windows

Se ocorrer um problema no sistema ou com o usuário, configure a rede para enviar uma mensagem automática a uma pessoa designada, como o administrador do sistema, no mesmo ou em outro computador.

- No computador de envio ou recepção, inicie o serviço Messenger no painel de controle do Windows Services.
- No computador de envio, inicie o serviço Alerta no painel de controle Windows Services.

Para mais informações sobre a criação de um objeto de alerta, consulte a documentação do Windows.

Licenciamento eletrônico 3

Para o software SCIEX OS, o licenciamento eletrônico pode ser bloqueado por nó ou baseado em servidor.

Para o software Central Administrator Console (CAC), apenas as licenças bloqueadas por nó estão disponíveis.

O ID de ativação pode ser obrigatória para solicitações futuras de serviço ou suporte. Para acessar o ID de ativação da licença bloqueada por nó ou baseada em servidor:

- No espaço de trabalho Configuration, clique em **Licenças** na janela SCIEX OS.

Nota: Renove a licença antes que ela expire. A licença do software CAC é anual.

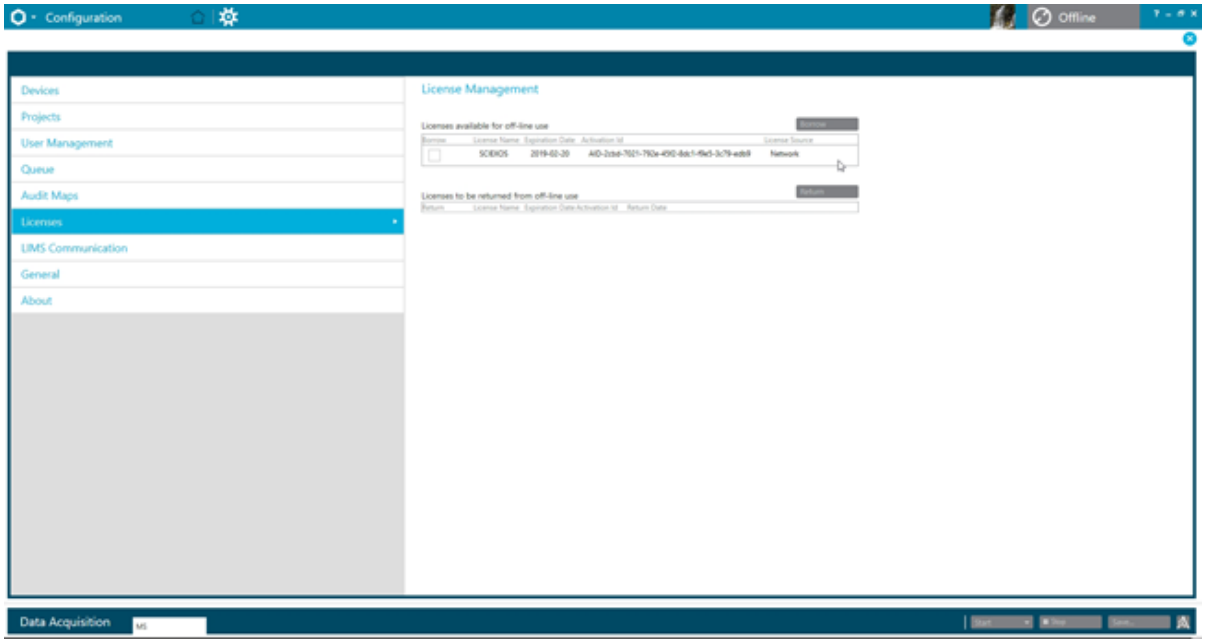
Empréstimo de uma licença eletrônica baseada em servidor

É necessária uma licença para utilizar o SCIEX OS. Se o licenciamento baseado em servidor estiver sendo usada, então os usuários que desejam trabalhar offline podem reservar uma licença para até 7 dias. Durante esse período, a licença eletrônica emprestada é específica do computador.

Nota: Esse procedimento não é aplicável para o software Central Administrator Console (CAC).

1. Abra o espaço de trabalho de Configuração.
2. Clique em **Licenças**.
   A tabela Licenças disponíveis para uso offline mostra todas as licenças disponíveis para empréstimo.

Figura 3-1: Gerenciamento de licenças: empréstimo de uma licença



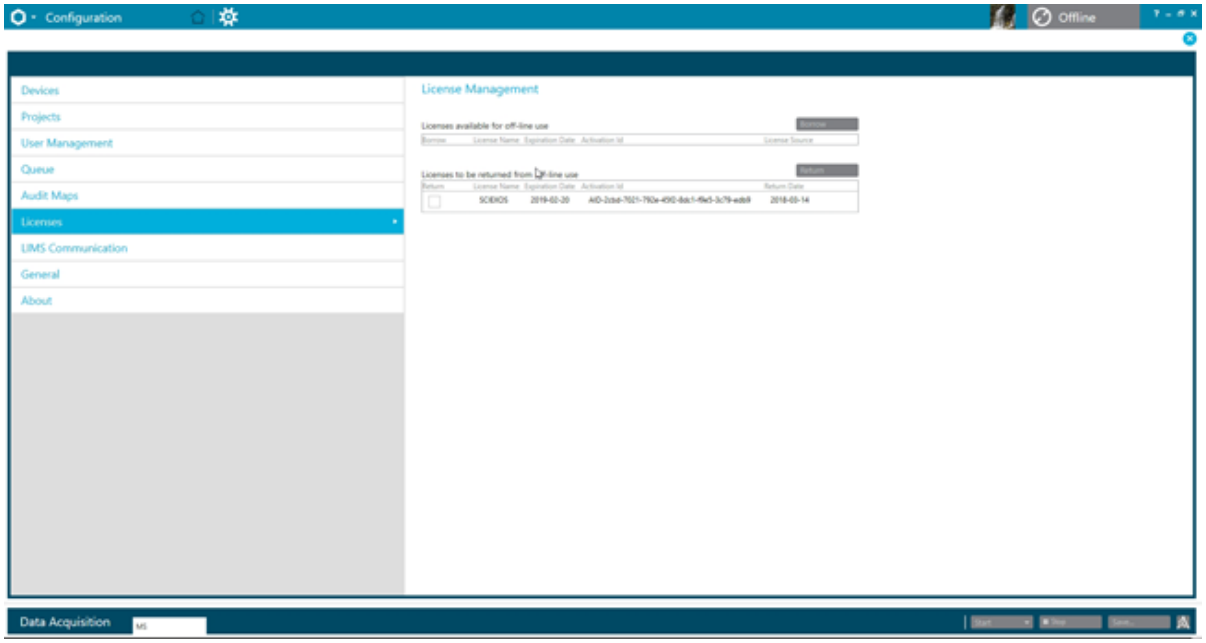
3. Selecione a licença a ser emprestada e, em seguida, clique em **Emprestar**.

Devolução de uma licença eletrônica baseada em servidor

Nota: Esse procedimento não é aplicável para o software Central Administrator Console (CAC).

1. Abra o espaço de trabalho de Configuração.
2. Clique em **Licenças**.
   A tabela Licenças a serem devolvidas do uso offline mostra todas as licenças que podem ser devolvidas, ou seja, todas as licenças emprestadas por este computador.

Figura 3-2: Gerenciamento de licenças: devolução de uma licença



3. Selecione a licença a ser devolvida e, em seguida, clique em **Retornar**.

Configuração de segurança do software Controle de acesso 4

Esta seção descreve como controlar o acesso ao software SCIEX OS. Para controlar o acesso ao software, o administrador executa as seguintes tarefas:

Nota: Para executar as tarefas desta seção, o usuário precisa ter privilégios de administrador local para a estação de trabalho na qual o software está sendo instalado.

- Instale e configure o software SCIEX OS.
- Adicione e configure usuários e funções.
- Configure o acesso aos projetos e arquivos de projeto no diretório raiz.

Este procedimento fornece instruções para a administração local do software SCIEX OS. Para uma administração centralizada do software SCIEX OS, consulte a seção: Console do administrador central.

Nota: Qualquer alteração à configuração do SCIEX OS entra em vigor após o SCIEX OS ser reiniciado.

Localização da informação de segurança

Todas as informações de segurança ficam armazenadas no computador local, na pasta `C:\ProgramData\SCIEX\Clearcore2.Acquisition`, em um arquivo chamado `Security.data`.

Fluxo de trabalho de segurança do software

O software SCIEX OS trabalha com componentes de auditoria de eventos de segurança, aplicativo e sistema das Ferramentas Administrativas do Windows.

Configure a segurança nos seguintes níveis:

- Autenticação do Windows: acesso ao computador.
- Autorização do Windows: acesso a arquivos e pastas.
- Autenticação do software SCIEX OS: capacidade de abrir o SCIEX OS.
- Autorização do software SCIEX OS: acesso à funcionalidade no SCIEX OS.

Para obter a lista de tarefas para configurar a segurança, consulte a tabela: Tabela 4-1. Para obter as opções de configuração dos vários níveis de segurança, consulte a tabela: Tabela 4-2.

Tabela 4-1: Fluxo de trabalho para configuração de segurança

Tarefa	Procedimento
Instale o software SCIEX OS.	Consulte o documento: *Guia do usuário do software SCIEX OS*.
Configure o acesso ao software SCIEX OS.	Consulte a seção: Configurar acesso ao software SCIEX OS.
Configurar a segurança de arquivos do Windows e NTFS.	Consulte a seção: Configurar o acesso ao projetos e arquivos do projeto.

Tabela 4-2: Opções de configuração de segurança

Opção	CFR 21 Part 11
Segurança do Windows	
Configurar usuários e grupos (autenticação).	Sim
Habilitar auditoria do Windows e auditoria de arquivos e diretório.	Sim
Definir as permissões do arquivo (autorização).	Sim
Instalação do software **SCIEX OS**	
Instale o software SCIEX OS.	Sim
Abra o Event Viewer para inspecionar a instalação.	Sim
Segurança do software	
Selecionar o modo de segurança.	Sim
Configure os usuários e funções no software SCIEX OS.	Sim
Configurar notificação por e-mail.	Sim
Criar modelos de mapa de auditoria e configurar mapas de rastreamentos de auditoria do projeto e da estação de trabalho.	Sim
Habilitar o recurso de soma de verificação para arquivos `wiff`.	Sim
Tarefas Comuns	
Adicionar novos projetos.	Sim

Instalação do software Instalar o software SCIEX OS

Antes de instalar o software SCIEX OS, leia estes documentos, disponíveis no DVD de instalação do software ou no pacote para download na Web: *Guia de instalação do software* e *Notas de versão*. É importante compreender a diferença entre um computador de processamento e um computador de aquisição e realizar a sequência de instalação correta.

Requisitos do sistema

Para obter os requisitos mínimos de instalação, consulte o documento: *Guia de instalação do software*.

Pré-configurar opções de auditoria

Para obter uma descrição dos mapas de auditoria instalados, consulte a seção: Modelos de mapas de auditoria instalados. Após a instalação, o administrador do software SCIEX OS pode criar mapas de auditoria personalizados e atribuir uma mapa de auditoria diferente no espaço de trabalho Configuração.

Configurar o Security Mode

Esta seção descreve as opções de Modo de segurança encontradas na página Gerenciamento de usuários na estação de trabalho Configuração.

Modo Integrado: se o usuário que estiver no momento com sessão iniciada no Windows for definido como um usuário no software, ele terá acesso ao software SCIEX OS.

Modo Misto: os usuários fazem logon no Windows e no software separadamente. As credenciais usadas para fazer logon no Windows não podem ser as mesmas usadas para fazer logon no SCIEX OS.. Use esse modo para permitir que um grupo de usuários façam logon no Windows com o mesmo conjunto de credenciais, mas requerem que cada usuário façam logon no software com credenciais únicas. Essas credenciais únicas podem ser atribuídas a uma função especificada, da mesma maneira que no modo Integrado.

Se Mixed Mode estiver selecionado, os recursos Screen Lock e Auto Logoff serão disponibilizados para uso.

Screen Lock e Auto Logoff: para fins de segurança, a tela do computador pode ser configurada para ser bloqueada após um período definido de inatividade. Um temporizador de logoff automático também pode ser definido, de modo que o software seja encerrado após ter sido bloqueado por um período definido. Screen Lock e Auto Logoff estão disponíveis apenas em Mixed Mode.

Nota: Quando a tela é bloqueada, a aquisição e o processamento continuam. O logoff automático não ocorrerá se o processamento estiver ocorrendo ou se a Results Table não tiver sido salva. Quando o usuário termina a sessão usando o encerramento de sessão forçado, todo o processamento para e todos os dados não salvos são perdidos. A aquisição continua após o usuário fazer logoff, de forma automática ou manual.

Security Notification: o software pode ser configurado para enviar automaticamente uma notificação por e-mail após uma quantidade configurável de falhas de logon em um período configurável, para avisar sobre as tentativas de acesso ao sistema por usuários não autorizados. A quantidade de falhas de logon pode ser de 3 a 7, e o período pode ser de 5 minutos a 24 horas.

Nota: Para grupos de trabalho administrados pelo software Central Administrator Console (CAC), o modo de segurança não pode ser gerenciado com o software SCIEX OS.

Selecionar o Security Mode

1. Abra o espaço de trabalho de Configuração.
2. Clique em **Gerenciamento de usuários**.
3. Clique na guia **Modo de segurança**.
4. Selecione **Modo integrado** ou **Modo misto**. Consulte a seção: Configurar o Security Mode.
5. Clique em **Salvar**.
   Aparece uma caixa de diálogo de confirmação.
6. Clique em **OK**.

Configurar opções de segurança da estação de trabalho (Mixed Mode)

Procedimentos de pré-requisito
• Defina o modo de segurança para Mixed Mode. Consulte a seção: Configurar o Security Mode.

Se Mixed Mode estiver selecionado, os recursos Screen Lock e Auto Logoff poderão ser configurados.

1. Abra o espaço de trabalho de Configuração.
2. Clique em **Gerenciamento de usuários**.
3. Abra a guia Modo de segurança.
4. Para configurar o recurso Screen Lock, siga as seguintes etapas:
   a. Selecione **Bloqueio de tela**.
   b. No campo **Aguarde**, especifique um tempo, em minutos.
      Se a estação de trabalho estiver inativa durante esse período, ela será automaticamente bloqueada. O usuário com sessão iniciada pode desbloquear a estação de trabalho inserindo as credenciais corretas ou o Administrador pode encerrar a sessão do usuário.
5. Para configurar o recurso Auto Logoff, siga as seguintes etapas:
   a. Selecione **Logoff automático**.
   b. No campo **Aguarde**, especifique um tempo, em minutos. Se a estação de trabalho tiver sido bloqueada durante esse período, de forma automática ou manual, o usuário que estiver com sessão iniciada terá sua sessão encerrada. Todos o processamento para. A aquisição, no entanto, continua.
6. Clique em **Salvar**.
   Uma caixa de diálogo de confirmação é aberta.

7. Clique em **OK**.

Configurar notificação por e-mail (Mixed Mode)

Procedimentos de pré-requisito
• Defina o modo de segurança para Mixed Mode. Consulte a seção: Configurar o Security Mode.

O software pode ser configurado para enviar uma mensagem de e-mail após um número configurável de erros de logon em um período configurável. O número de falhas de logon pode ser de 3 a 7, e o período de 5 minutos a 24 horas.

O computador com o software instalado deve ser capaz de comunicar-se com um servidor SMTP com uma porta aberta.

1. Abra o espaço de trabalho de Configuração.
2. Clique em **Gerenciamento de usuários**.
3. Abra a guia Modo de segurança.
4. Marque a caixa de seleção **Enviar mensagens de e-mail após** e, em seguida, especifique quantas falhas de logon dentro de que período, em minutos, irão gerar uma notificação de e-mail.

   Dica! Para desabilitar as notificações, desmarque a caixa de seleção **Enviar mensagens de e-mail após**.

5. No campo **Servidor SMTP**, digite o nome do servidor SMTP.

   Nota: A conta SMTP envia e-mail ao servidor de e-mail. O servidor SMTP é definido no aplicativo de e-mail corporativo.

6. No campo **Número da porta**, digite o número da porta aberta.
   Clique em **Aplicar padrão** para inserir o número da porta padrão, 25.
7. No campo **Até**, digite o endereço de e-mail para o qual a mensagem deve ser enviada. Por exemplo: nomedeusuário@domínio.com.
8. No campo **De**, digite o endereço de e-mail a ser mostrado no campo **De** da mensagem.
9. No campo **Assunto**, digite o assunto da mensagem.
10. No campo **Mensagem**, digite o texto a ser incluído no corpo da mensagem.
11. Clique em **Salvar**.
    Uma caixa de diálogo de confirmação é aberta.
12. Clique em **OK**.
13. Para verificar a configuração, clique em **Enviar mensagem de teste**.

Configurar acesso ao software SCIEX OS

Antes de configurar a segurança, faça o seguinte:

- Remova todos os usuários e grupos de usuários desnecessários como replicador, usuário power e operador de backup do computador local e da rede.

  Nota: Cada computador SCIEX é configurado com uma conta local com nível de administrador, **abservice**. Essa conta é usada pelo serviço e suporte técnico da SCIEX para instalar o sistema, fazer sua manutenção e suporte. Não remova ou desative essa conta. Se a conta tiver que ser removida ou desativada, prepare um plano alternativo para acesso da SCIEX e comunique-o ao FSE local.

- Adicione grupos de usuários que contêm grupos que não terão tarefas administrativas.
- Configure as permissões do sistema.
- Crie procedimentos e políticas de conta adequados para usuários em Group Policy.

Consulte a documentação do Windows para obter mais informações sobre:

- Usuários e grupos e usuários do Active Directory.
- Políticas de senha e bloqueio de conta para contas de usuários.
- Política de direitos do usuário.

Quando usuários trabalham em um ambiente de diretório ativo, as configurações de política de grupo de diretório ativo afetam a segurança do computador. Discuta as políticas de grupo com o administrador do Active Directory como parte de uma implementação completa do software SCIEX OS.

SCIEX OS Permissões

Figura 4-1: Página User Management

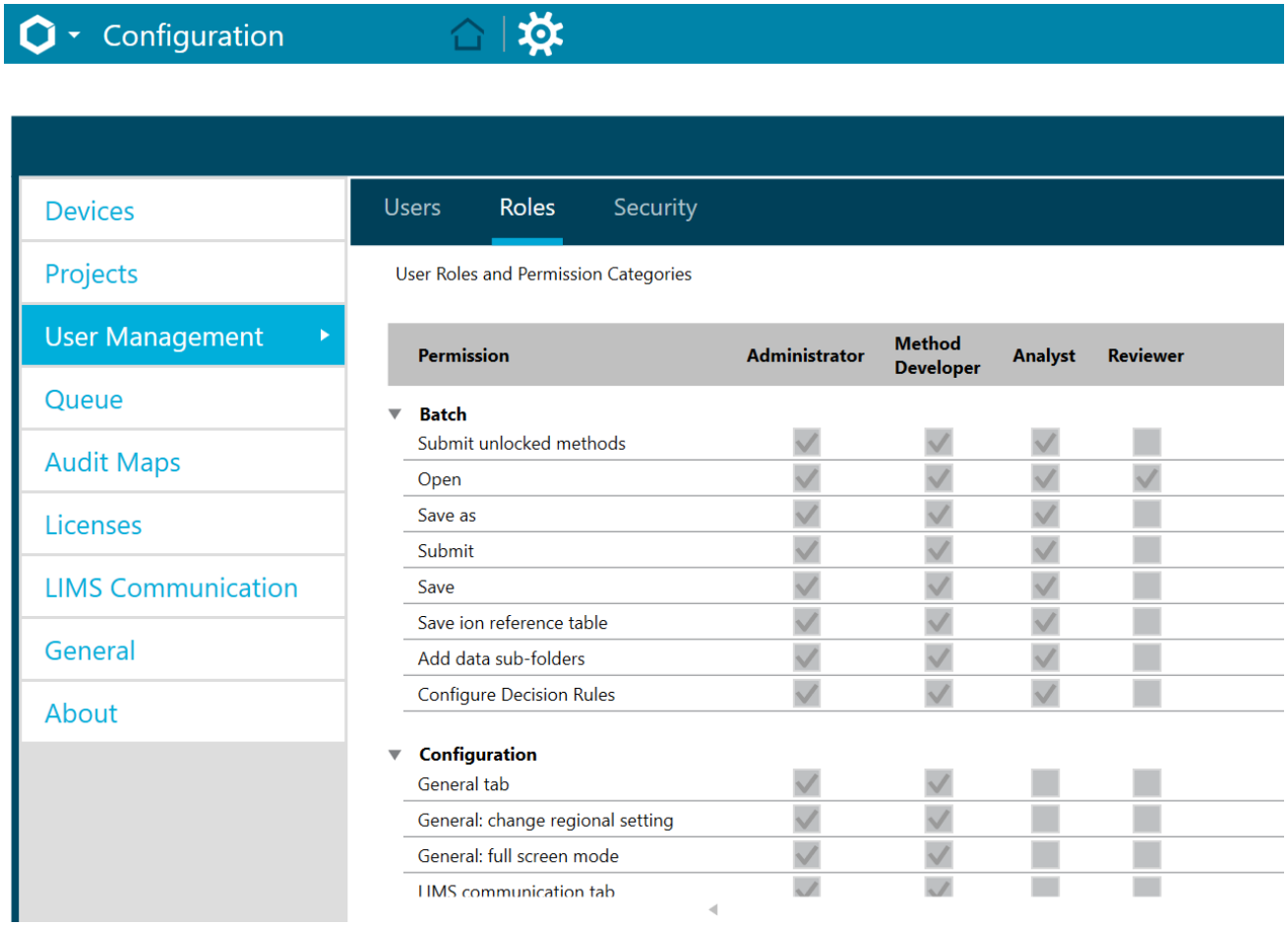


Tabela 4-3: Permissões

Permissão	Descrição
Lote	
Enviar métodos desbloqueados	Permite que os usuários enviem lotes que contenham métodos desbloqueados.
Abrir	Permite que os usuários abram lotes existentes.
Salvar como	Permite que os usuários salvem lotes com um novo nome.
Enviar	Permite que os usuários enviem lotes.
Salvar	Permite que os usuários salvem um lote e sobrescrevam o conteúdo existente.
Saltar tabela de referência de íons	Permite que os usuários editem a tabela de referência de íons.

Tabela 4-3: Permissões (continuação)

Permissão	Descrição
Adicionar subpastas de dados	Permite que os usuários criem subpastas para armazenamento de dados.
Configurar regras de decisão	Permite que os usuários adicionem e alterem regras de decisão.
Configuração	
Guia Geral	Permite que os usuários abram a página Geral no espaço de trabalho Configuração.
Geral: alterar a configuração regional	Permite que os usuários apliquem as configurações regionais ativas do sistema no software SCIEX OS.
Geral: modo de tela inteira	Permite que os usuários habilitem e desabilitem o modo de tela cheia.
Geral: interromper serviços do Windows	Permite que os usuários habilitem e desabilitem a opção **Configurações do Windows**.
Guia Comunicação LIMS	Permite que os usuários abram a página Comunicação LIMS no espaço de trabalho Configuração.
Guia Mapas de auditoria	Permite que os usuários abram a página Mapas de auditoria no espaço de trabalho Configuração.
Guia Fila	Permite que os usuários abram a página Fila no espaço de trabalho Configuração.
Fila: tempo de ociosidade do instrumento	Permite que os usuários definam o tempo ocioso do instrumento.
Fila: número máx. de amostras adquiridas	Permite que os usuários definam o número máximo permitido de amostras adquiridas.
Fila: outras configurações de fila	Permite que os usuários configurem outras definições da fila.
Guia Projetos	Permite que os usuários abram a página Projetos no espaço de trabalho Configuração.
Projetos: criar projeto	Permite que usuários criem projetos.
Projetos: aplicar um modelo de mapa de auditoria a um projeto existente	Permite que os usuários apliquem um mapa de auditoria a um projeto.
Projetos: criar diretório raiz	Permite que os usuários criem um diretório raiz para armazenamento de projetos.
Projetos: definir diretório raiz atual	Permite que os usuários alterem o diretório raiz de um projeto.

Tabela 4-3: Permissões (continuação)

Permissão	Descrição
Projetos: especificar credenciais da rede	Permite que os usuários especifiquem uma conta de rede segura (SNA) para ser usada durante a aquisição de rede se o usuário conectado não tiver acesso ao recurso da rede.
Projetos: habilitar a gravação da soma de verificação para criação de dados wiff	Permite que os usuários configurem o software para gravar somas de verificação em arquivos de dados `wiff`.
Projetos: apagar diretório raiz	Permite que os usuários excluam um diretório raiz da lista.
Guia Dispositivos	Permite que os usuários abram a página Dispositivos no espaço de trabalho Configuração.
Guia Gerenciamento de usuários	Permite que os usuários abram a página Gerenciamento de usuários no espaço de trabalho Configuração.
Forçar logoff do usuário	Permite que os usuários forcem um usuário conectado ao software SCIEX OS a fazer logoff.
Guia CAC [1]	Permite que os usuários abram a página CAC no espaço de trabalho Configuração.
Guia Modelos de impressão	Permite que os usuários abram a guia Imprimir modelos no espaço de trabalho Configuração.
Modelos de impressão: crie e modifique modelos de impressão	Permite que os usuários criem novos modelos de impressão ou alterem os modelos de impressão existentes.
Modelos de impressão: defina o modelo de impressão padrão	Permite que os usuários tornem o modelo de impressão ativo o padrão para o projeto ativo.
Modelos de impressão: aplique o modelo atual a todos os projetos no diretório raiz	Permite que os usuários adicionem o modelo de impressão à lista de modelos de impressão disponíveis para projetos selecionados em um diretório raiz definido.
Log de eventos	
Acessar espaço de trabalho do registro de eventos	Permite que os usuários abram o espaço de trabalho Registro de eventos.
Arquivar registro	Permite que os usuários arquivem os logs no espaço de trabalho Registro de eventos.

[1] Na versão 3.1, a permissão **Habilitar administração central** foi renomeada para **CAC**. A página CAC do espaço de trabalho Configuração pode ser usada para configurar a administração central do software SCIEX OS.

Tabela 4-3: Permissões (continuação)

Permissão	Descrição
Rastreamento de auditoria	
Acessar espaço de trabalho do rastreamento de auditoria	Permite que os usuários abram o espaço de trabalho Rastreamento de auditoria.
Visualizar mapa de auditoria ativo	Permite que os usuários vejam os mapas de auditoria ativos de uma estação de trabalho ou projeto no espaço de trabalho Audit Trail.
Imprimir/Exportar rastreamento de auditoria	Permite que os usuários imprimam ou exportem os rastreamentos de auditoria.
Painel de aquisição de dados	
Start (Iniciar)	Permite que os usuários iniciem a aquisição no painel Aquisição de dados.
Parar	Permite que os usuários parem a aquisição no painel Aquisição de dados.
Salvar	Permite que os usuários salvem dados adquiridos com outro nome de arquivo no painel Aquisição de dados.
Método de MS e LC	
Acessar espaço de trabalho Method	Permite que os usuários abram os espaços de trabalho Método de MS e Método de LC.
Novo	Permite que os usuários criem métodos MS e LC.
Abrir	Permite que os usuários abram métodos MS e LC.
Salvar	Permite que os usuários salvem um método e sobrescrevam o conteúdo existente.
Salvar como	Permite que os usuários salvem métodos com um novo nome.
Bloquear/Desbloquear método	Permite que os usuários bloqueiem métodos, para evitar edição, e desbloqueiem métodos.
Fila	
Gerenciar	Permite que os usuários abram o espaço de trabalho Fila.
Iniciar/Parar	Permite que os usuários iniciem ou interrompam a fila.
Imprimir	Permite que os usuários imprimam a fila.
Editar amostra	Permite que os usuários alterem o nome ou o arquivo de dados de uma amostra.
Biblioteca	

Tabela 4-3: Permissões (continuação)

Permissão	Descrição
Acessar espaço de trabalho Library	Permite que os usuários abram o espaço de trabalho Biblioteca. Não aplicável ao fluxo de trabalho de quantificação.
Ajuste de MS	
Acessar espaço de trabalho Ajuste MS	Permite que os usuários abram o espaço de trabalho Ajuste de MS.
Ajuste MS avançado	Sistemas X500 QTOF e ZenoTOF 7600: permite que os usuários acessem as opções de ajuste avançadas, incluindo **Otimização do detector**, **Ajuste TOF positivo**, **Ajuste TOF negativo**, **Ajuste de unidade Q1 positiva**, **Ajuste de unidade Q1 negativa**, **Ajuste alto de Q1 positivo** e **Ajuste alto de Q1 negativo**.
Resolução de problemas avançada	Permite que os usuários abram a caixa de diálogo Resolução de problemas avançada.
Verificação rápida de status	Sistemas X500 QTOF e ZenoTOF 7600: permite que os usuários façam a **Verificação rápida de status positivo** e a **Verificação rápida de status negativo**.
Restaurar dados do instrumento	Permite que os usuários restaurem as configurações de ajuste salvas anteriormente.
Explorador	
Acessar espaço de trabalho Explorer	Permite que os usuários abram o espaço de trabalho Explorador.
Exportar	Permite que os usuários exportem dados do espaço de trabalho Explorador.
Imprimir	Permite que os usuários imprimam dados no espaço de trabalho Explorador.
Opções	Permite que os usuários alterem as opções do espaço de trabalho Explorador.
Recalibrar	Permite que os usuários recalibrem amostras e espectros no espaço de trabalho Explorador. Não aplicável ao fluxo de trabalho de quantificação.
Analytics	
Novos resultados	Permite que os usuários criem tabelas de resultados.
Criar método de processamento	Permite que os usuários criem métodos de processamento.
Modificar método de processamento	Permite que os usuários alterem métodos de processamento.

Tabela 4-3: Permissões (continuação)

Permissão	Descrição
Permitir a exportação e criar relatório de Tabela de resultados desbloqueada	Permite que os usuários exportem ou gerem um relatório de uma tabela de resultados ou de estatísticas, se a tabela de resultados não estiver bloqueada.
Salvar resultados para o lote de automação	Permite que tabelas de resultados criadas automaticamente no espaço de trabalho Lote sejam salvas. Essa permissão é necessária para autoprocessamento durante a aquisição.
Alterar algoritmo de integração de método de quantificação padrão	Permite que os usuários alterem a algoritmo de integração nas configurações padrão do projeto.
Alterar parâmetros de integração de método de quantificação padrão	Permite que os usuários alterem os parâmetros de integração nas configurações padrão do projeto.
Habilitar aviso de pico modificado do projeto	Permite que os usuários habilitem a propriedade de aviso de pico modificado para um projeto.
Adicionar amostras	Permite que os usuários adicionem amostras a uma tabela de resultados.
Remover amostras selecionadas	Permite que os usuários removam amostras de uma tabela de resultados.
Exportar, importar ou remover calibração externa	Permite que os usuários exportem, importem ou removam calibrações externas.
Modificar nome da amostra	Permite que os usuários alterem o nome da amostra na tabela de resultados.
Modificar tipo da amostra	Permite que os usuários alterem o tipo da amostra na tabela de resultados. Os tipos válidos de amostra são: padrão, controle de qualidade e desconhecido.
Modificar ID da amostra	Permite que os usuários alterem o ID da amostra na tabela de resultados.
Modificar concentração real	Permite que os usuários alterem a concentração real das amostras padrão e QC na tabela de resultados.
Modificar fator de diluição	Permite que os usuários alterem o fator de diluição na tabela de resultados.

Tabela 4-3: Permissões (continuação)

Permissão	Descrição
Modificar campos de comentário	Permite que os usuários alterem os seguintes campos de comentário: • **Comentário do componente** • **Comentário de IS** • **Comentário de pico de IS** • **Comentário de pico** • **Comentário de amostra**
Habilitar integração manual	Permite que os usuários realizem a integração manual.
Definir pico como não encontrado	Permite que os usuários definam um pico como **Não encontrado**.
Incluir ou excluir um pico da tabela de resultados	Permite que os usuários incluam e excluam picos da tabela de resultados.
Opções de regressão	Permite que os usuários alterem opções de regressão no painel Curva de calibração.
Modificar parâmetros de integração da tabela de resultados para um único cromatograma	Permite que os usuários alterem parâmetros de integração de um cromatograma único no painel Peak Review.
Modificar o método quantitativo para o componente da tabela de resultados	Permite que os usuários selecionem um método de processamento diferente para um componente do painel Peak Review com a opção **Atualizar método de processamento para o componente**.
Criar novas configurações de gráfico métrico	Permite que os usuários criem novos gráficos de métrica e alterem as configurações.
Adicionar colunas personalizadas	Permite que os usuários adicionem colunas personalizadas a uma tabela de resultados.
Definir formato de título de análise de pico	Permite que os usuários alterem o título da revisão de pico.
Remover coluna personalizada	Permite que os usuários removam colunas personalizadas de uma tabela de resultados.
Configurações de exibição da Tabela de resultados	Permite que os usuários personalizem as colunas exibidas na tabela de resultados.
Bloquear tabela de resultados	Permite que os usuários bloqueiem a tabela de resultados para prevenir edição.

Tabela 4-3: Permissões (continuação)

Permissão	Descrição
Desbloquear tabela de resultados	Permite que os usuários desbloqueiem uma tabela de resultados para permitir alterações.
Marcar arquivo de resultados como revisado e salvar	Permite que os usuários marquem a tabela de resultados como revisada e salvem a tabela.
Modificar modelo de relatório	Permite que os usuários alterem modelos de relatório.
Transferir resultados para o LIMS	Permite que os usuários façam upload dos resultados para um Sistema de gerenciamento de informações laboratoriais (LIMS).
Modificar coluna do código de barras	Permite que os usuários alterem a coluna **Código de barras** na tabela de resultados.
Alterar atribuição da amostra de comparação	Permite que os usuários alterem a amostra de comparação especificada na coluna **Comparação** da tabela de resultados.
Adicionar espectros de MS/MS à biblioteca	Permite que os usuários adicionem a uma biblioteca os espectros MS/MS selecionados. Não aplicável ao fluxo de trabalho de quantificação.
Configurações padrão do projeto	Permite que os usuários alterem as configurações de processamento quantitativas e qualitativas do projeto padrão.
Criar relatórios em todos os formatos	Permite que os usuários criem relatórios em todos os formatos. Usuários sem essa permissão podem gerar relatórios somente no formato PDF.
Editar parâmetros dos critérios de alerta	Permite que os usuários alterem os parâmetros de sinalização em um método de processamento.
Alteração do parâmetro de remoção automática do valor discrepante	Permite que os usuários alterem os parâmetros para a remoção automática de valores discrepantes.
Habilitar remoção automática do valor discrepante	Permite que os usuários alterem o método de processamento para ativar o recurso de remoção automática de valor discrepante.
Atualizar método de processamento FF/LS	Permite que os usuários usem o Formula Finder e a Pesquisa na biblioteca para atualizar métodos de processamento. Não aplicável ao fluxo de trabalho de quantificação.

Tabela 4-3: Permissões (continuação)

Permissão	Descrição
Atualizar resultados via FF/LS	Permite que os usuários usem o Formula Finder e a Pesquisa na biblioteca para atualizar os resultados. Não aplicável ao fluxo de trabalho de quantificação.
Habilitar agrupamento por funcionalidade de adutos	Permite que os usuários atualizem o método de processamento para usar o recurso de agrupamento por adutos.
Buscar arquivos	Permite que os usuários naveguem fora da pasta local de dados.
Habilitar adição padrão	Permite que os usuários atualizem o método de processamento para ativar o recurso de adição padrão.
Definir regra de porcentagem de integração manual	Permite que os usuários alterem o parâmetro **Integração manual %**.
Modificar peso/volume	Permite que os usuários alterem o campo **Peso/volume**.

Sobre usuários e funções

No software SCIEX OS, o administrador pode adicionar usuários e grupos do Windows ao banco de dados de gerenciamento de usuários. Para acessarem o software, os usuários devem ser definidos no banco de dados de gerenciamento de usuários ou serem membros de um grupo definido no banco de dados.

Os usuários podem ser atribuídos a uma ou mais funções predefinidas, mostradas na tabela a seguir, ou a funções personalizadas, se necessário. As funções às quais o usuário tem acesso estão especificadas por funções de usuário. As funções de usuário predefinidas não podem ser excluídas e suas permissões não podem ser modificadas.

Nota: Para os grupos de trabalho administrados pelo software Central Administrator Console (CAC), as páginas Gerenciamento de usuários serão somente leitura.

Tabela 4-4: Funções predefinidas

Função	Tarefas típicas
Administrador	• Gerencia o sistema • Configura a segurança
Desenvolvedor de método	• Cria métodos • Executa lotes • Analisa dados para uso do usuário

Tabela 4-4: Funções predefinidas (continuação)

Função	Tarefas típicas
Analista	• Executa lotes • Analisa dados para uso do usuário
Revisor	• Revisa os dados • Revisa rastreamentos de auditoria • Revisa os resultados quantitativos

Tabela 4-5: Permissões predefinidas

Permissão	Administrador	Desenvolvedor de método	Analista	Revisor
Lote				
Enviar métodos desbloqueados	✓	✓	✓	×
Abrir	✓	✓	✓	✓
Salvar como	✓	✓	✓	×
Enviar	✓	✓	✓	×
Salvar	✓	✓	✓	×
Saltar tabela de referência de íons	✓	✓	✓	×
Adicionar subpastas de dados	✓	✓	✓	×
Configurar regras de decisão	✓	✓	✓	×
Configuração				
Guia Geral	✓	✓	×	×
Geral: alterar a configuração regional	✓	✓	×	×
Geral: modo de tela inteira	✓	✓	×	×
Geral: interromper serviços do Windows	✓	×	×	×
Guia Comunicação LIMS	✓	✓	×	×

Tabela 4-5: Permissões predefinidas (continuação)

Permissão	Administrador	Desenvolvedor de método	Analista	Revisor
Guia Mapas de auditoria	✓	×	×	×
Guia Fila	✓	✓	✓	✓
Fila: tempo de ociosidade do instrumento	✓	✓	×	×
Fila: número máx. de amostras adquiridas	✓	✓	×	×
Fila: outras configurações de fila	✓	✓	×	×
Guia Projetos	✓	✓	✓	✓
Projetos: criar projeto	✓	✓	✓	×
Projetos: aplicar um modelo de mapa de auditoria a um projeto existente	✓	×	×	×
Projetos: criar diretório raiz	✓	×	×	×
Projetos: definir diretório raiz atual	✓	×	×	×
Projetos: especificar credenciais da rede	✓	×	×	×
Projetos: habilitar a gravação da soma de verificação para criação de dados wiff	✓	×	×	×
Projetos: apagar diretório raiz	✓	×	×	×
Guia Dispositivos	✓	✓	✓	×
Guia Gerenciamento de usuários	✓	×	×	×
Forçar logoff do usuário	✓	×	×	×
Guia CAC[1]	✓	×	×	×

Tabela 4-5: Permissões predefinidas (continuação)

Permissão	Administrador	Desenvolvedor de método	Analista	Revisor
Guia Modelos de impressão	✓	✓	×	×
Modelos de impressão: crie e modifique modelos de impressão	✓	✓	×	×
Modelos de impressão: defina o modelo de impressão padrão	✓	✓	×	×
Modelos de impressão: aplique o modelo atual a todos os projetos no diretório raiz	✓	×	×	×
Log de eventos				
Acessar espaço de trabalho do registro de eventos	✓	✓	✓	✓
Arquivar registro	✓	✓	✓	✓
Rastreamento de auditoria				
Acessar espaço de trabalho do rastreamento de auditoria	✓	✓	✓	✓
Visualizar mapa de auditoria ativo	✓	✓	✓	✓
Imprimir/Exportar rastreamento de auditoria	✓	✓	✓	✓
Painel de aquisição de dados				
Start (Iniciar)	✓	✓	✓	×
Parar	✓	✓	✓	×

[1] Na versão 3.1, a permissão **Habilitar administração central** foi renomeada para **CAC**. A página CAC do espaço de trabalho Configuração pode ser usada para configurar a administração central do software SCIEX OS.

Tabela 4-5: Permissões predefinidas (continuação)

Permissão	Administrador	Desenvolvedor de método	Analista	Revisor
Salvar	✓	✓	✓	×
Método de MS e LC				
Acessar espaço de trabalho Method	✓	✓	✓	✓
Novo	✓	✓	×	×
Abrir	✓	✓	✓	✓
Salvar	✓	✓	×	×
Salvar como	✓	✓	×	×
Bloquear/ Desbloquear método	✓	✓	×	×
Fila				
Gerenciar	✓	✓	✓	×
Iniciar/Parar	✓	✓	✓	×
Imprimir	✓	✓	✓	✓
Editar amostra	✓	✓	×	×
Biblioteca				
Acessar espaço de trabalho Library	✓	✓	✓	✓
Ajuste de MS				
Acessar espaço de trabalho Ajuste MS	✓	✓	✓	×
Ajuste MS avançado	✓	✓	×	×
Resolução de problemas avançada	✓	✓	×	×
Verificação rápida de status	✓	✓	✓	×
Restaurar dados do instrumento	✓	✓	×	×
Explorador				
Acessar espaço de trabalho Explorer	✓	✓	✓	✓

Tabela 4-5: Permissões predefinidas (continuação)

Permissão	Administrador	Desenvolvedor de método	Analista	Revisor
Exportar	✓	✓	✓	×
Imprimir	✓	✓	✓	×
Opções	✓	✓	✓	×
Recalibrar	✓	✓	×	×
Analytics				
Novos resultados	✓	✓	✓	×
Criar método de processamento	✓	✓	✓	×
Modificar método de processamento	✓	✓	×	×
Permitir a exportação e criar relatório de Tabela de resultados desbloqueada	✓	×	×	×
Salvar resultados para o lote de automação	✓	✓	✓	×
Alterar algoritmo de integração de método de quantificação padrão	✓	✓	×	×
Alterar parâmetros de integração de método de quantificação padrão	✓	✓	×	×
Habilitar aviso de pico modificado do projeto	✓	×	×	×
Adicionar amostras	✓	✓	✓	×
Remover amostras selecionadas	✓	✓	✓	×
Exportar, importar ou remover calibração externa	✓	✓	✓	×

Tabela 4-5: Permissões predefinidas (continuação)

Permissão	Administrador	Desenvolvedor de método	Analista	Revisor
Modificar nome da amostra	✓	✓	✓	×
Modificar tipo da amostra	✓	✓	✓	×
Modificar ID da amostra	✓	✓	✓	×
Modificar concentração real	✓	✓	✓	×
Modificar fator de diluição	✓	✓	✓	×
Modificar campos de comentário	✓	✓	✓	×
Habilitar integração manual	✓	✓	✓	×
Definir pico como não encontrado	✓	✓	✓	×
Incluir ou excluir um pico da tabela de resultados	✓	✓	✓	×
Opções de regressão	✓	✓	✓	×
Modificar parâmetros de integração da tabela de resultados para um único cromatograma	✓	✓	✓	×
Modificar o método quantitativo para o componente da tabela de resultados	✓	✓	✓	×
Criar novas configurações de gráfico métrico	✓	✓	✓	✓
Adicionar colunas personalizadas	✓	✓	✓	×
Definir formato de título de análise de pico	✓	×	×	×

Tabela 4-5: Permissões predefinidas (continuação)

Permissão	Administrador	Desenvolvedor de método	Analista	Revisor
Remover coluna personalizada	✓	✓	×	×
Configurações de exibição da Tabela de resultados	✓	✓	✓	✓
Bloquear tabela de resultados	✓	✓	✓	✓
Desbloquear tabela de resultados	✓	×	×	×
Marcar arquivo de resultados como revisado e salvar	✓	×	×	✓
Modificar modelo de relatório	✓	✓	×	×
Transferir resultados para o LIMS	✓	✓	✓	×
Modificar coluna do código de barras	✓	✓	×	×
Alterar atribuição da amostra de comparação	✓	✓	×	×
Adicionar espectros de MS/MS à biblioteca	✓	✓	×	×
Configurações padrão do projeto	✓	✓	×	×
Criar relatórios em todos os formatos	✓	✓	✓	✓
Editar parâmetros dos critérios de alerta	✓	✓	✓	×
Alteração do parâmetro de remoção automática do valor discrepante	✓	✓	×	×
Habilitar remoção automática do valor discrepante	✓	✓	✓	×

Tabela 4-5: Permissões predefinidas (continuação)

Permissão	Administrador	Desenvolvedor de método	Analista	Revisor
Atualizar método de processamento FF/LS	✓	✓	×	×
Atualizar resultados via FF/LS	✓	✓	×	×
Habilitar agrupamento por funcionalidade de adutos	✓	✓	×	×
Buscar arquivos	✓	✓	✓	✓
Habilitar adição padrão	✓	✓	✓	×
Definir regra de porcentagem de integração manual	✓	×	×	×
Modificar peso/ volume	✓	✓	✓	×

Gerenciar usuários

Adicionar um usuário ou grupo

1. Abra o espaço de trabalho de Configuração.
2. Abra a página Gerenciamento de usuários.
3. Abra a guia Usuários.
4. Clique em **Adicionar usuário** ( ).
   A caixa de diálogo Selecionar usuário ou grupo é aberta.
5. Digite o nome de um usuário ou grupo e, em seguida, clique em **OK**.

   Dica! Para obter informações sobre a caixa de diálogo Selecionar usuário ou grupo e como usá-la, pressione **F1**.
6. Para tornar o usuário ativo, marque a caixa de seleção **Usuário ou grupo ativo**.
7. Na área **Funções**, selecione uma ou mais funções e, em seguida, clique em **Salvar**.

Desativar usuários ou grupos

1. Abra o espaço de trabalho de Configuração.

2. Abra a página Gerenciamento de usuários.
3. Abra a guia Usuários.
4. Na lista **Nome de usuário ou grupo**, selecione o usuário ou grupo a ser desativado.
5. Desmarque a caixa de seleção **Usuário ou grupo ativo**.
   O software pede confirmação.
6. Clique em **Sim**.

Remover usuários ou grupos

Use esse procedimento para remover um usuário ou grupo do software. Se um usuário ou grupo for removido do sistema Windows, ele também precisará ser excluído do software SCIEX OS.

1. Abra o espaço de trabalho de Configuração.
2. Abra a página Gerenciamento de usuários.
3. Abra a guia Usuários.
4. Na lista **Nome de usuário ou grupo**, selecione o usuário ou grupo a ser removido.
5. Clique em **Excluir**.
   O software pede confirmação.
6. Clique em **OK**.

Gerenciar funções

Alteração das funções atribuídas a um usuário ou grupo

Use este procedimento para atribuir novas funções a um usuário ou grupo ou remover atribuições de função existentes.

1. Abra o espaço de trabalho de Configuração.
2. Abra a página Gerenciamento de usuários.
3. Abra a guia Usuários.
4. No campo **Nome de usuário ou grupo**, selecione o usuário ou grupo a ser alterado.
5. Selecione as funções a serem atribuídas ao usuário ou grupo e apague as funções a serem removidas.
6. Clique em **Salvar**.

Criar uma função personalizada

1. Abra o espaço de trabalho de Configuração.
2. Abra a página Gerenciamento de usuários.
3. Abra a guia Funções.
4. Clique em **Adicionar função** ().

A caixa de diálogo Duplicar a função de um usuário é aberta.

5. No campo **Função do usuário existente**, selecione a função a ser usada como modelo para a nova função.
6. Insira um nome e uma descrição para a função e, em seguida, clique em **OK**.
7. Selecione os privilégios de acesso da função.
8. Clique em **Salvar todas as funções**.
9. Clique em **OK**.

Excluir uma função personalizada

Nota: Se o usuário for atribuído somente à função que está sendo excluída, o sistema solicitará a exclusão do usuário, bem como da função.

1. Abra o espaço de trabalho de Configuração.
2. Abra a página Gerenciamento de usuários.
3. Abra a guia Funções.
4. Clique em **Excluir uma função**.
   A caixa de diálogo Excluir função de um usuário é aberta.
5. Selecione a função a ser excluída e, em seguida, clique em **OK**.

Exportar e importar configurações de gerenciamento do usuário

O banco de dados de gerenciamento de usuários do software SCIEX OS pode ser exportado e importado. Após configurar o banco de dados Gerenciamento do usuário em um computador SCIEX, por exemplo, exporte-o e, em seguida, importe-o em outros computadores SCIEX para certificar-se de que as configurações de gerenciamento do usuário são consistentes.

Somente usuários de domínio são exportados. Usuários locais não são exportados.

Antes de importar as configurações de gerenciamento do usuário, o software faz backup automaticamente das configurações atuais. O usuário pode restaurar o último backup.

Exportar configurações de gerenciamento do usuário

1. Abra o espaço de trabalho de Configuração.
2. Abra a página Gerenciamento de usuários.
3. Clique em **Avançado** > **Exportar configurações de Gerenciamento do usuário**.
   A caixa de diálogo Exportar configurações de gerenciamento do usuário é aberta.
4. Clique em **Navegar**.
5. Busque e selecione a pasta que em que as configurações serão salvas e, em seguida, clique em **Selecione a pasta**.

6. Clique em **Exportar**.
   Uma mensagem de confirmação é mostrada, com o nome do arquivo que contém as configurações exportadas.
7. Clique em **OK**.

Importar configurações de gerenciamento do usuário

1. Abra o espaço de trabalho de Configuração.
2. Abra a página Gerenciamento de usuários.
3. Clique em **Avançado** > **Importar configurações de gerenciamento do usuário**.
   A caixa de diálogo Importar configurações de gerenciamento do usuário é aberta.
4. Clique em **Navegar**.
5. Busque e selecione o arquivo que contém as configurações a serem importadas; em seguida, clique em **Abrir**.
   O software verifica que o arquivo é válido.
6. Clique em **Importar**.
   O software realiza o backup das configurações de gerenciamento do usuário atuais e importa as novas configurações. Aparece uma mensagem de confirmação.
7. Clique em **OK**.

Restaurar configurações de gerenciamento do usuário

Antes de importar as configurações de gerenciamento de usuários, o software faz backup das configurações atuais. Use este procedimento para restaurar o último backup das configurações de gerenciamento do usuário.

1. Abra o espaço de trabalho de Configuração.
2. Abra a página Gerenciamento de usuários.
3. Clique em **Avançado** > **Restaurar as configurações anteriores**.
   A caixa de diálogo Restaurar configurações de gerenciamento do usuário é aberta.
4. Clique em **Sim**.
5. Feche o software SCIEX OS e abra-o novamente.

Configurar o acesso ao projetos e arquivos do projeto

Use os recursos de segurança do Windows para controlar o acesso à pasta `SCIEX OS Data`. Por padrão, os arquivos de projeto são armazenados na pasta `SCIEX OS Data`. Para acessar um projeto, os usuários precisam ter acesso ao diretório raiz no qual os dados do projeto estão armazenados. Para obter mais informações, consulte a seção: Configuração da Segurança do Windows.

Pastas de projeto

Cada projeto contém pastas que armazenam diferentes tipos de arquivo. Para obter informações sobre o conteúdo das diferentes pastas, consulte a tabela: Tabela 4-6.

Tabela 4-6: Pastas de projeto

Pasta	Contents
\Acquisition Methods	Contém os métodos espectrômetro de massas (MS) e LC que foram criados no projeto. Os métodos MS possuem a extensão msm e os métodos LC possuem a extensão LCM.
\Audit Data	Contém o mapa de auditoria de projeto e todos os registros de auditoria.
\Batch	Contém todos os arquivos do lote de aquisição que foram salvos. Os lotes de aquisição têm a extensão bch.
\Data	Contém os arquivos de dados de aquisição. Os arquivos dos dados de aquisição possuem extensões wiff e wiff2.
\Project Information	Contém os arquivos das configurações padrão do projeto.
\Quantitation Methods	Contém todos os arquivos do método de processamento. Os métodos de processamento têm a extensão qmethod.
\Quantitation Results	Contém todos os arquivos da Tabela de resultados de quantificação. Os arquivos de tabelas de resultados têm a extensão qsession.

Tipos de arquivos de software

Para ver os tipos de arquivo comuns no software SCIEX OS, consulte a tabela: Tabela 4-7.

Tabela 4-7: arquivos do SCIEX OS

Extensão	Tipo de arquivo	Pasta
atds	• Dados e arquivos do rastreamento de auditoria da estação de trabalho • Configurações de rastreamento de auditoria da estação de trabalho • Dados e arquivos do rastreamento de auditoria do projeto • Configurações de rastreamento de auditoria de projeto	• Para projetos: *<project name>*\Audit Data • Para a estação de trabalho: C:\ProgramData\SCIEX\Audit Data

Tabela 4-7: arquivos do SCIEX OS (continuação)

Extensão	Tipo de arquivo	Pasta
atms	Mapas de auditoria	• Para projetos: <*project name*>\Audit Data • Para a estação de trabalho: C:\ProgramData\SCIEX\Audit Data
bch	Batch	Batch
cset	Configurações da Tabela de resultados	Project Information
dad	Arquivo de dados de espectrometria de massas	• Optimization • Data
exml	Configurações padrão do projeto	Project Information
journal	Arquivos temporários criados pelo software SCIEX OS	Várias pastas
lcm	Método LC	Acquisition Methods
msm	Método MS	Acquisition Methods
pdf	Dados de documento portátil	—
qlayout	Layout do espaço de trabalho	— **Nota:** O layout do espaço de trabalho padrão para um projeto é armazenado na pasta Project Information.
qmethod	Método de processamento	Quantitation Methods
qsession	Tabela de resultados do software Tabela de resultados **Nota:** o software SCIEX OS só pode abrir arquivos qsession que foram criados com o SCIEX OS.	Quantitation Results
wiff	Arquivo de dados de espectrometria de massas compatível com o SCIEX OS **Nota:** o software SCIEX OS cria arquivos wiff e wiff2.	Data

Tabela 4-7: arquivos do SCIEX OS (continuação)

Extensão	Tipo de arquivo	Pasta
`wiff.scan`	Arquivo de dados de espectrometria de massas	• `Optimization` • `Data`
`wiff2`	Arquivo de dados de espectrometria de massas gerado pelo software SCIEX OS	• `Optimization` • `Data`
`xls` ou `xlsx`	Planilha Excel	`Batch`
`xps`	Recalibração	`Data\Cal`

Console do administrador central 5

O software Central Administrator Console (CAC) é uma alternativa opcional para a administração local com o software SCIEX OS. O software CAC contém gerenciamento e personalização de função central, usuários, estações de trabalho e grupos de trabalho, tudo em um só aplicativo.

Esta seção descreve o software CAC e explica como configurar e usá-lo para gerenciar centralmente pessoas, projetos e estações de trabalho.

Nota: Para usar o software CAC e registrar estações de trabalho no servidor, certifique-se de que o software SCIEX OS está instalado em cada estação de trabalho.

O software CAC está habilitado para licença e pode ser instalado em qualquer estação de trabalho compatível com o a versão 3.0 do SCIEX OS e o Windows Server 2019.

O software CAC faz parte de um pacote do instalador do SCIEX OS. No entanto, os softwares CAC e SCIEX OS não podem ser instalados na mesma estação de trabalho.

Usuários

Use a página Gerenciamento de usuários para adicionar usuários e grupos do Windows ao banco de dados de gerenciamento de usuários do software SCIEX OS. O administrador também pode adicionar, modificar e excluir funções do usuário na seção User Roles and Permissions. Para acessar o software, os usuários devem ser definidos no banco de dados User Management, ou deverão ser um membro de um grupo definido no banco de dados.

Pool de usuários

Somente usuários autorizados podem fazer login na estação de trabalho e acessar o software SCIEX OS quando SCIEX OS é gerenciado com o software Central Administrator Console (CAC). Antes que os usuários possam ser adicionados a grupos de trabalho, eles devem ser adicionados ao pool de usuários.

Adicionar um usuário ou grupo ao pool de usuários

1. Abra o espaço de trabalho do Administração central.
2. Abra a página Gerenciamento de usuários.
3. Abra a guia Pool de usuários.
4. Clique em **Adicionar usuários ao pool de usuários** ( ).
   A caixa de diálogo Selecionar usuários ou grupos é aberta.
5. Digite o nome de um usuário ou grupo e, em seguida, clique em **OK**.

Dica! Mantenha pressionada a tecla **Ctrl** e, em seguida, clique em **OK** para selecionar vários usuários ou grupos.

Excluir usuários ou grupos

1. Abra o espaço de trabalho do Administração central.
2. Abra a página Gerenciamento de usuários.
3. Abra a guia Pool de usuários.
4. No painel direito, selecione o usuário ou grupo a ser excluído e, em seguida, clique em **Excluir**.
   O software pede confirmação.
5. Clique em **OK**.

Funções e permissões do usuário

Esta seção descreve a página Funções e permissões do usuário.

Os usuários podem ser atribuídos a uma ou mais funções predefinidas, descritas na tabela a seguir, ou a funções personalizadas, se necessário. As funções às quais o usuário tem acesso estão especificadas por funções de usuário. As funções predefinidas não podem ser excluídas e suas permissões não podem ser alteradas.

Nota: No software Central Administrator Console (CAC), os usuários também podem ver a versão mais antiga do software SCIEX OS na qual a permissão é suportada.

Tabela 5-1: Funções predefinidas

Função	Tarefas típicas
Administrador	• Gerencia o sistema • Configura a segurança
Desenvolvedor de método	• Cria métodos • Executa lotes • Analisa dados para uso do usuário
Analista	• Executa lotes • Analisa dados para uso do usuário
Revisor	• Revisa os dados • Revisa rastreamentos de auditoria • Revisa os resultados quantitativos

Tabela 5-2: Permissões predefinidas

Permissão	Administrador	Desenvolvedor de método	Analista	Revisor
Lote				
Enviar métodos desbloqueados	✓	✓	✓	×
Abrir	✓	✓	✓	✓
Salvar como	✓	✓	✓	×
Enviar	✓	✓	✓	×
Salvar	✓	✓	✓	×
Saltar tabela de referência de íons	✓	✓	✓	×
Adicionar subpastas de dados	✓	✓	✓	×
Configurar regras de decisão	✓	✓	✓	×
Configuração				
Guia Geral	✓	✓	×	×
Geral: alterar a configuração regional	✓	✓	×	×
Geral: modo de tela inteira	✓	✓	×	×
Guia Comunicação LIMS	✓	✓	×	×
Geral: interromper serviços do Windows	✓	×	×	×
Guia Mapas de auditoria	✓	×	×	×
Guia Fila	✓	✓	✓	✓
Fila: tempo de ociosidade do instrumento	✓	✓	×	×
Fila: número máx. de amostras adquiridas	✓	✓	×	×
Fila: outras configurações de fila	✓	✓	×	×

Tabela 5-2: Permissões predefinidas (continuação)

Permissão	Administrador	Desenvolvedor de método	Analista	Revisor
Guia Projetos	✓	✓	✓	✓
Projetos: criar projeto	✓	✓	✓	×
Projetos: aplicar um modelo de mapa de auditoria a um projeto existente	✓	×	×	×
Projetos: criar diretório raiz	✓	×	×	×
Projetos: definir diretório raiz atual	✓	×	×	×
Projetos: especificar credenciais da rede	✓	×	×	×
Projetos: habilitar a gravação da soma de verificação para criação de dados wiff	✓	×	×	×
Projetos: apagar diretório raiz	✓	×	×	×
Guia Dispositivos	✓	✓	✓	×
Guia Gerenciamento de usuários	✓	×	×	×
Forçar logoff do usuário	✓	×	×	×
Guia CAC[1]	✓	×	×	×
Guia Modelos de impressão	✓	✓	×	×
Modelos de impressão: crie e modifique modelos de impressão	✓	✓	×	×

[1] Na versão 3.1, a permissão **Habilitar administração central** foi renomeada para **CAC**. A página CAC do espaço de trabalho Configuração pode ser usada para configurar a administração central do software SCIEX OS.

Tabela 5-2: Permissões predefinidas (continuação)

Permissão	Administrador	Desenvolvedor de método	Analista	Revisor
Modelos de impressão: defina o modelo de impressão padrão	✓	✓	×	×
Modelos de impressão: aplique o modelo atual a todos os projetos no diretório raiz	✓	×	×	×
Log de eventos				
Acessar espaço de trabalho do registro de eventos	✓	✓	✓	✓
Arquivar registro	✓	✓	✓	✓
Rastreamento de auditoria				
Acessar espaço de trabalho do rastreamento de auditoria	✓	✓	✓	✓
Visualizar mapa de auditoria ativo	✓	✓	✓	✓
Imprimir/Exportar rastreamento de auditoria	✓	✓	✓	✓
Painel de aquisição de dados				
Start (Iniciar)	✓	✓	✓	×
Parar	✓	✓	✓	×
Salvar	✓	✓	✓	×
Método de MS e LC				
Acessar espaço de trabalho Method	✓	✓	✓	✓
Novo	✓	✓	×	×
Abrir	✓	✓	✓	✓
Salvar	✓	✓	×	×

Tabela 5-2: Permissões predefinidas (continuação)

Permissão	Administrador	Desenvolvedor de método	Analista	Revisor
Salvar como	✓	✓	×	×
Bloquear/ Desbloquear método	✓	✓	×	×
Fila				
Gerenciar	✓	✓	✓	×
Iniciar/Parar	✓	✓	✓	×
Imprimir	✓	✓	✓	✓
Editar amostra	✓	✓	×	×
Biblioteca				
Acessar espaço de trabalho Library	✓	✓	✓	✓
Ajuste de MS				
Acessar espaço de trabalho Ajuste MS	✓	✓	✓	×
Ajuste MS avançado	✓	✓	×	×
Resolução de problemas avançada	✓	✓	×	×
Verificação rápida de status	✓	✓	✓	×
Restaurar dados do instrumento	✓	✓	×	×
Analytics				
Novos resultados	✓	✓	✓	×
Criar método de processamento	✓	✓	✓	×
Modificar método de processamento	✓	✓	×	×
Permitir a exportação e criar relatório de Tabela de resultados desbloqueada	✓	×	×	×

Tabela 5-2: Permissões predefinidas (continuação)

Permissão	Administrador	Desenvolvedor de método	Analista	Revisor
Salvar resultados para o lote de automação	✓	✓	✓	×
Alterar algoritmo de integração de método de quantificação padrão	✓	✓	×	×
Alterar parâmetros de integração de método de quantificação padrão	✓	✓	×	×
Habilitar aviso de pico modificado do projeto	✓	×	×	×
Adicionar amostras	✓	✓	✓	×
Remover amostras selecionadas	✓	✓	✓	×
Exportar, importar ou remover calibração externa	✓	✓	✓	×
Modificar nome da amostra	✓	✓	✓	×
Modificar tipo da amostra	✓	✓	✓	×
Modificar ID da amostra	✓	✓	✓	×
Modificar concentração real	✓	✓	✓	×
Modificar fator de diluição	✓	✓	✓	×
Modificar campos de comentário	✓	✓	✓	×
Habilitar integração manual	✓	✓	✓	×
Definir pico como não encontrado	✓	✓	✓	×

Tabela 5-2: Permissões predefinidas (continuação)

Permissão	Administrador	Desenvolvedor de método	Analista	Revisor
Incluir ou excluir um pico da tabela de resultados	✓	✓	✓	×
Opções de regressão	✓	✓	✓	×
Modificar parâmetros de integração da tabela de resultados para um único cromatograma	✓	✓	✓	×
Modificar o método quantitativo para o componente da tabela de resultados	✓	✓	✓	×
Criar novas configurações de gráfico métrico	✓	✓	✓	✓
Adicionar colunas personalizadas	✓	✓	✓	×
Definir formato de título de análise de pico	✓	×	×	×
Remover coluna personalizada	✓	✓	×	×
Configurações de exibição da Tabela de resultados	✓	✓	✓	✓
Bloquear tabela de resultados	✓	✓	✓	✓
Desbloquear tabela de resultados	✓	×	×	×
Marcar arquivo de resultados como revisado e salvar	✓	×	×	✓
Modificar modelo de relatório	✓	✓	×	×
Transferir resultados para o LIMS	✓	✓	✓	×

Tabela 5-2: Permissões predefinidas (continuação)

Permissão	Administrador	Desenvolvedor de método	Analista	Revisor
Modificar coluna do código de barras	✓	✓	×	×
Alterar atribuição da amostra de comparação	✓	✓	×	×
Adicionar espectros de MS/MS à biblioteca	✓	✓	×	×
Configurações padrão do projeto	✓	✓	×	×
Criar relatórios em todos os formatos	✓	✓	✓	✓
Editar parâmetros dos critérios de alerta	✓	✓	✓	×
Alteração do parâmetro de remoção automática do valor discrepante	✓	✓	×	×
Habilitar remoção automática do valor discrepante	✓	✓	✓	×
Atualizar método de processamento FF/LS	✓	✓	×	×
Atualizar resultados via FF/LS	✓	✓	×	×
Habilitar agrupamento por funcionalidade de adutos	✓	✓	×	×
Buscar arquivos	✓	✓	✓	✓
Habilitar adição padrão	✓	✓	✓	×
Definir regra de porcentagem de integração manual	✓	×	×	×
Modificar peso/ volume	✓	✓	✓	×
Explorador				

Tabela 5-2: Permissões predefinidas (continuação)

Permissão	Administrador	Desenvolvedor de método	Analista	Revisor
Acessar espaço de trabalho Explorer	✓	✓	✓	✓
Exportar	✓	✓	✓	×
Imprimir	✓	✓	✓	×
Opções	✓	✓	✓	×
Recalibrar	✓	✓	×	×

Adicionar uma função personalizada

O software Central Administrator Console (CAC) possui quatro funções predefinidas. Se forem necessárias funções adicionais, copie uma função existente e atribua os direitos de acesso.

1. Abra o espaço de trabalho do Administração central.
2. Abra a página Gerenciamento de usuários.
3. Abra a guia Funções e permissões do usuário.
4. Clique em **Adicionar função** ().
   A caixa de diálogo Duplicar a função de um usuário é aberta.
5. No campo **Função do usuário existente**, selecione a função a ser usada como modelo para a nova função.
6. Insira um nome e uma descrição para a função e, em seguida, clique em **OK**.
   A nova função é mostrada no campo Funções do usuário e categorias de permissão.
7. Selecione os privilégios de acesso para a função marcando as caixas de seleção adequadas.
8. Clique em **Salvar todas as funções**.

Excluir uma função personalizada

1. Abra o espaço de trabalho do Administração central.
2. Abra a página Gerenciamento de usuários.
3. Abra a guia Funções e permissões do usuário.
4. Clique em **Excluir uma função**.
   A caixa de diálogo Excluir função de um usuário é aberta.
5. Selecione a função a ser excluída e, em seguida, clique em **OK**.

Grupos de trabalho

Use a página Gerenciamento de grupos de trabalho para gerenciar grupos de trabalho. Grupos de trabalho possuem usuários, estações de trabalho e projetos.

Crie um grupo de trabalho adicionando recursos de seus respectivos pools. Antes de criar um grupo de trabalho, certifique-se de adicionar todos os usuários em potencial ao Pool de usuários, as estações de trabalho ao Pool de estações de trabalho e os diretórios raiz do projeto ao Pool de projetos.

Se for necessário, adicione funções adicionais. Opcionalmente, selecione o modo de segurança para cada grupo de trabalho.

A configuração do modo de segurança para o grupo de trabalho prevalece sobre a configuração do modo de segurança para a estação de trabalho se a estação de trabalho for registrada no software Central Administrator Console (CAC) e se for um membro do grupo de trabalho.

Não adicione usuários locais a grupos de trabalho. O software CAC é um aplicativo de rede e apenas os usuários de rede devem ser adicionados a um grupo de trabalho.

Nota: Em cada grupo de trabalho, pelo menos a um usuário deve ser atribuída a função de administrador. Somente um administrador ou supervisor pode desbloquear a tela do software CAC se o usuário logado no momento estiver indisponível.

Se a segurança baseada em servidor não for mais necessária em uma determinada estação de trabalho, gerencie a segurança da estação de trabalho localmente com o software SCIEX OS.

Criar um grupo de trabalho

1. Abra o espaço de trabalho do Administração central.
2. Abra a página Gerenciamento de grupos de trabalho.
3. Clique em **Adicionar um grupo de trabalhos** ( ).
   A caixa de diálogo Adicionar a um grupo de trabalhos é aberta.
4. Digite um nome no campo **Nome do grupo de trabalho**.
5. Digite uma descrição no campo **Descrição** e clique em **Adicionar**.
   O grupo de trabalho é criado e adicionado ao painel Gerenciar grupos de trabalho e atribuições. O software Central Administrator Console (CAC) cria o nome apropriado do grupo de trabalho no servidor.

   Nota: O modo Integrado é a configuração de segurança padrão.

Excluir um grupo de trabalho

Se um grupo de trabalho não for mais necessário, exclua-o da lista de grupos de trabalho. Excluir um grupo de trabalho apenas exclui o grupo de trabalho do software Central Administrator Console (CAC). Nenhum dado é perdido da estação de trabalho.

1. Abra o espaço de trabalho do Administração central.
2. Abra a página Gerenciamento de grupos de trabalho.
3. Expanda a lista **Grupos de trabalho** e encontre o grupo de trabalho a ser excluído. Clique em **Excluir**.
   A caixa de diálogo Excluir grupos de trabalho é aberta.
4. Clique em **Sim**.

Adicionar usuários ou grupos a um grupo de trabalho

Nota: Usuários adicionados ao grupo de trabalho não são atribuídos automaticamente a uma função. Para atribuir funções aos usuários, consulte a seção: Adicionar ou remover uma função.

1. Abra o espaço de trabalho do Administração central.
2. Abra a página Gerenciamento de grupos de trabalho.
3. No painel Gerenciar grupos de trabalho e atribuições, expanda o grupo de trabalho a ser alterado e, em seguida, expanda a lista **Usuários**.
4. Selecione um usuário ou grupo e, em seguida, clique em **Adicionar** ().

   Dica! Adicione ou selecione vários usuários pressionando **Shift** e selecionando os usuários desejados.

   O usuário ou grupo é adicionado ao grupo de trabalho atual.
5. Atribua uma ou mais funções ao usuário ou grupo adicionado. Consulte a seção: Adicionar ou remover uma função.
6. Clique em **Salvar**.

Adicionar ou remover uma função

Procedimentos de pré-requisito
• Adicionar usuários ou grupos a um grupo de trabalho.

Para obter informações sobre criar funções no software Central Administrator Console (CAC), consulte a seção: Adicionar uma função personalizada. Usuários ou grupos com uma função atribuída possuem todas as permissões associadas à função. Usuários ou grupos podem ter mais de uma função por vez.

1. Abra o espaço de trabalho do Administração central.

2. Abra a página Gerenciamento de grupos de trabalho.
3. No painel Gerenciar grupos de trabalho e atribuições, expanda o grupo de trabalho a ser alterado e, em seguida, expanda a lista **Usuários**.
4. Na seção Associação atual do grupo de trabalho, atribua ou remova funções na coluna **Atribuir funções**.
5. Clique em **Salvar**.

Adicionar estações de trabalho a um grupo de trabalho

Nota: Uma estação de trabalho é exibida no pool de estações de trabalho apenas se tiver sido registrada no software Central Administrator Console (CAC). Consulte a seção: Adicione uma estação de trabalho

1. Abra o espaço de trabalho do Administração central.
2. Abra a página Gerenciamento de grupos de trabalho.
3. No painel Gerenciar grupos de trabalho e atribuições, expanda o grupo de trabalho a ser alterado e, em seguida, expanda a lista **Estações de trabalho**.
4. Selecione uma estação de trabalho e, em seguida, clique em **Adicionar** (). A estação de trabalho é adicionada ao grupo de trabalho atual.
5. Clique em **Salvar**.

Atribuir configurações de segurança do grupo de trabalho

Procedimentos de pré-requisito
• Adicione uma estação de trabalho • Adicionar estações de trabalho a um grupo de trabalho

Para obter informações sobre os modos de segurança, consulte a seção: Configurar o Security Mode.

1. Abra o espaço de trabalho do Administração central.
2. Abra a página Gerenciamento de grupos de trabalho.
3. No painel Gerenciar grupos de trabalho e atribuições, expanda o grupo de trabalho a ser alterado e, em seguida, expanda a lista **Estações de trabalho**.
4. (Opcional) Para tornar o grupo de trabalho atual o grupo de trabalho padrão para essa estação de trabalho, marque a caixa de seleção **Configurar padrão** na seção Associação atual do grupo de trabalho.
5. Na seção Atribuir configurações de segurança, selecione o **Modo de segurança** para o grupo de trabalho e, em seguida, digite os tempos de **Bloqueio de tela** e **Logoff automático** apropriados.
6. Clique em **Salvar**.

Adicionar projetos a um grupo de trabalho

Nota: Esse procedimento é necessário somente se o acesso ao projeto for gerenciado de forma centralizada.

Nota: Se um projeto é adicionado a mais de um grupo de trabalho, o acesso do usuário ao projeto é adicionado e não substituído. Por exemplo, o Grupo de Trabalho 1 tem o Usuário A, o Usuário B e o Projeto_01. O Grupo de Trabalho 2 tem o Usuário B e o Usuário C. Se o Projeto_01 for adicionado ao Grupo de Trabalho 2, o Usuário A, Usuário B e Usuário C terão acesso ao Projeto_01.

1. Abra o espaço de trabalho do Administração central.
2. Abra a página Gerenciamento de grupos de trabalho.
3. No painel Gerenciar grupos de trabalho e atribuições, expanda o grupo de trabalho a ser alterado e, em seguida, expanda a lista **Projetos**.
4. Marque a caixa de seleção **Usar configurações centrais para projetos**.
   A seção de seleção de projetos é exibida.
5. Selecione um **Diretório raiz do projeto** para adicionar um grupo de projetos inteiro ou expanda a raiz do projeto e selecione um projeto específico para adicionar ao grupo de trabalho.
6. Clique em **Adicionar** () para adicionar os projetos ao grupo de trabalho.
   A raiz do projeto é adicionada à tabela Associação atual do grupo de trabalho. Expanda a raiz do projeto para exibir os projetos atuais no grupo de trabalho.
7. Clique em **Salvar**.

Gerenciar projetos

Use a página Gerenciamento de projetos para criar, modificar e excluir projetos.

Para acessar um projeto, os usuários precisam ter acesso ao diretório raiz no qual os dados do projeto estão armazenados. Para obter mais informações, consulte a seção: Sobre projetos e diretórios raiz.

Sobre projetos e diretórios raiz

Um diretório raiz é uma pasta que contém um ou mais projetos. É a pasta em que o software procura os dados do projeto. O diretório raiz predefinido é `D:\SCIEX OS Data`.

Para se certificar de que as informações do projeto estão armazenadas em segurança, crie projetos usando o software Central Administrator Console (CAC). Adicione projetos ao Pool raiz do projeto antes de adicioná-los ao grupo de trabalho. Consulte a seção: Adicionar um projeto.

Os dados do projeto podem ser organizados em subpastas. Crie as subpastas com o software CAC. Consulte a seção: Adicionar uma subpasta.

Nota: Se um projeto é criado fora do software CAC, a raiz do projeto deve ser atualizada após o projeto ser criado. Quando a raiz é atualizada, o conteúdo do Pool raiz do projeto é sincronizado com o conteúdo das raízes do projeto na rede.

Adicionar um diretório raiz

Diretório raiz é a pasta em que um ou mais projetos são armazenados.

Nota: O software salva até dez diretórios raízes.

Dica! Os drives locais não são acessíveis na rede. Um diretório raiz pode ser criado somente em uma unidade compartilhada.

1. Abra o espaço de trabalho do Administração central.
2. Abra a página Gerenciamento de projetos.
3. Clique em **Adicionar raiz do projeto nova ou atual ao pool de projetos** ().
   A caixa de diálogo Adicionar diretório raiz é aberta.
4. Digite o caminho completo da pasta do diretório raiz e, em seguida, clique em **OK**.
   A pasta é criada.

   Dica! Em vez de digitar o caminho, clique em **Navegar** e, em seguida, selecione a pasta em que o diretório raiz será criado.

   Dica! Em alternativa, crie uma pasta no File Explorer e, em seguida, vá até lá e selecione a pasta.

   Nota: Para instalações do software SCIEX OS com uma licença de processamento, o diretório raiz pode ser uma pasta do software Analyst (`Analyst Data\Projects`).
5. Clique em **OK**.
   O novo diretório raiz torna-se o diretório raiz para o projeto atual.

Exclua o diretório raiz de um projeto

O software mantém uma lista dos últimos dez diretórios raízes que foram usados. O usuário pode excluir os diretórios raízes dessa lista.

Nota: Excluir o diretório raiz de um projeto também exclui todos os projetos associados do pool raiz do projeto.

1. Abra o espaço de trabalho do Administração central.
2. Abra a página Gerenciamento de projetos.
3. Procure o diretório raiz do projeto a ser excluído e, em seguida, clique em **Excluir raiz do projeto**, na seção Ações.
   O software pede confirmação.

4. Clique em **OK**.

Adicionar um projeto

Procedimentos de pré-requisito
• Adicionar um diretório raiz

O projeto armazena métodos de aquisição, dados, lotes, métodos de processamento, resultados de processamento etc. Recomendamos o uso de uma pasta de projeto separada para cada um.

Não crie projetos nem copie ou cole arquivos fora do software Central Administrator Console (CAC).

1. Abra o espaço de trabalho do Administração central.
2. Abra a página Gerenciamento de projetos.
3. Clique em **Adicionar projeto**, na seção Ações da pasta raiz.
   A caixa de diálogo Novo projeto é aberta.
4. Digite o nome do projeto.
5. Clique em **OK**.
   O novo projeto é mostrado sob a raiz do projeto.

Adicionar uma subpasta

Os dados do projeto podem ser organizados em subpastas.

1. Abra o espaço de trabalho do Administração central.
2. Abra a página Gerenciamento de projetos.
3. Clique em **Adicionar subpastas de dados**, na seção Ações da pasta raiz.
   A caixa de diálogo Adicionar subpastas de dados é aberta.
4. Selecione um projeto para ao qual a subpasta pertencerá.
5. Clique em **Adicionar uma nova subpasta de dados** ().
   A caixa de diálogo Nome da subpasta de dados é aberta.
6. Digite o nome da subpasta.
7. Clique em **Salvar**.

   Dica! As subpastas podem ser aninhadas em outras subpastas. Para criar uma subpasta aninhada, selecione uma subpasta existente na seção Subpastas de dados do projeto e, em seguida, clique em **Adicionar uma nova subpasta de dados** ().
8. Feche a caixa de diálogo Adicionar subpastas de dados.

Estações de trabalho

Use a página Gerenciamento de estações de trabalho para gerenciar todas as estações de trabalho conectadas ao software CAC. As configurações personalizadas são aplicadas automaticamente às estações de trabalho sob o controle do software CAC.

Adicione uma estação de trabalho

Na página Gerenciamento de estações de trabalho, os administradores podem adicionar ou remover estações de trabalho e habilitar ou desabilitar o controle central de estações de trabalho.

1. Abra o espaço de trabalho do Administração central.
2. Abra a página Gerenciamento de estações de trabalho.
3. Clique em **Adicionar estação de trabalho ao pool de estações de trabalho** ().
   A caixa de diálogo Selecionar computadores é aberta.
4. Digite os nomes das estações de trabalho a serem adicionadas e, em seguida, clique em **OK**.
   O **Status** da administração central da estação de trabalho muda de **Conectando** para **Desabilitado**.
5. (Opcional) Para ativar o controle central da estação de trabalho:
   a. Na coluna **Status**, clique em **Desabilitado**.
   b. Clique em **OK**.

Dica! Os usuários podem também habilitar a administração central no software SCIEX OS software. Consulte o documento: *Sistema de ajuda do software SCIEX OS*.

Excluir uma estação de trabalho

Se uma estação de trabalho não estiver mais em uso ou não for mais parte de um grupo de trabalho, exclua-a do pool de estação de trabalho. Se uma estação de trabalho for excluída, ela será removida dos grupos de trabalho aos quais está atribuída. Nenhum dado é perdido na estação de trabalho quando ela é removida.

1. Abra o espaço de trabalho do Administração central.
2. Abra a página Gerenciamento de estações de trabalho.
3. Clique em **Gerenciamento da estação de trabalho**.
4. No painel Pool de estações de trabalho, procure a estação de trabalho a ser excluída e, em seguida, clique em **Excluir**.
   A caixa de diálogo Excluir estação de trabalho é aberta.
5. Clique em **OK**.

Recursos de relatórios e segurança

Gerar relatórios de dados

Siga este procedimento para gerar relatórios de dados que incluem detalhes como usuários configurados, funções, estações de trabalho, projetos e grupos de trabalho.

1. Abra o espaço de trabalho do Administração central.
2. Clique em **Imprimir**.
   A caixa de diálogo Opções de impressão é aberta.
3. Selecionar as páginas para imprimir e depois clique em **Continuar**.
4. Defina as opções de impressão e, em seguida, clique em **Imprimir**.
5. (Imprimir somente em PDF) Navegue até a localização em que o Relatório será salvo e, em seguida, clique em **Salvar**.

Exportar configurações do software CAC

Use este procedimento para exportar as configurações de segurança e tornar possível a importação em um outro sistema Central Administrator Console (CAC). As configurações são exportadas como um arquivo `ecac`.

1. Abra o espaço de trabalho do Administração central.
2. Clique em **Avançado** > **Exportar configurações CAC**.
   A caixa de diálogo Exportar configurações CAC é aberta.
3. Clique em **Navegar**.
4. Busque e selecione a pasta que em que as configurações serão salvas e, em seguida, clique em **Selecione a pasta**.
5. Clique em **Exportar**.
   Uma mensagem de confirmação é mostrada, com o nome do arquivo que contém as configurações exportadas.
6. Clique em **OK**.

Importar configurações do software CAC

Procedimentos de pré-requisito
• Exportar configurações do software CAC

Use este procedimento para importar configurações de segurança de outros sistemas Central Administrator Console (CAC). As configurações são importadas de um arquivo `ecac`.

1. Abra o espaço de trabalho do Administração central.
2. Abra o espaço de trabalho de Configuração.

3. Abra a página Gerenciamento de usuários.
4. Clique em **Avançado** > **Importar configurações CAC**.
   A caixa de diálogo Importar configurações CAC é aberta.
5. Clique em **Navegar**.
6. Busque e selecione o arquivo que contém as configurações a serem importadas; em seguida, clique em **Abrir**.
   O software verifica que o arquivo é válido.
7. Clique em **Importar**.
   O software realiza o backup das configurações atuais e importa as novas configurações. Aparece uma mensagem de confirmação.

   Nota: As configurações importadas são aplicadas após o software ser reiniciado.
8. Clique em **OK**.

Restaurar configurações do software CAC

Siga este procedimento para importar automaticamente as últimas configurações de `ecac` exportadas.

1. Abra o espaço de trabalho do Administração central.
2. Clique em **Avançado** > **Restaurar configurações CAC**.
   A caixa de diálogo Restaurar configurações CAC é aberta.

   Nota: As configurações restauradas são aplicadas após o software Central Administrator Console (CAC) ser reiniciado.
3. Clique em **Sim**.

Exportar configurações de gerenciamento do usuário CAC

Siga este procedimento para exportar as configurações de gerenciamento de usuários que podem ser aplicadas a outro sistema Central Administrator Console (CAC). As configurações são exportadas como um arquivo `data`.

Nota: As configurações exportadas só podem ser importadas para um sistema usando a mesma versão do software CAC.

1. Abra o espaço de trabalho Gerenciamento de configuração.
2. Clique em **Avançado** > **Exportar configurações de Gerenciamento do usuário**.
   A caixa de diálogo Exportar configurações CAC é aberta.
3. Clique em **Navegar**.
4. Busque e selecione a pasta que em que as configurações serão salvas e, em seguida, clique em **Selecione a pasta**.
5. Clique em **Exportar**.

Uma mensagem de confirmação é mostrada, com o nome do arquivo que contém as configurações exportadas.

6. Clique em **OK**.

Importar configurações do gerenciamento de usuários do CAC

Procedimentos de pré-requisito
• Exportar configurações de gerenciamento do usuário CAC

Siga este procedimento para importar configurações de segurança de outro sistema Central Administrator Console (CAC). As configurações são importadas de um arquivo `data`.

Nota: As configurações exportadas só podem ser importadas para um sistema usando a mesma versão do software CAC.

1. Abra o espaço de trabalho Gerenciamento de configuração.
2. Clique em **Avançado** > **Importar configurações de gerenciamento do usuário**.
   A caixa de diálogo Importar configurações de gerenciamento do usuário é aberta.
3. Clique em **Navegar**.
4. Busque e selecione o arquivo que contém as configurações a serem importadas; em seguida, clique em **Abrir**.
   O software verifica que o arquivo é válido.
5. Clique em **Importar**.
   O software realiza o backup das configurações atuais e importa as novas configurações. Aparece uma mensagem de confirmação.

   Nota: As configurações importadas são aplicadas após o software CAC ser reiniciado.

6. Clique em **OK**.

Aquisição de rede 6

Esta seção descreve como a aquisição de rede funciona no software SCIEX OS e os benefícios e limitações de projetos com base na rede. Também contém procedimentos para configuração da aquisição de rede.

Sobre aquisição de rede

A aquisição de rede pode ser usada para adquirir dados de um ou mais instrumentos em pastas do projeto com base na rede que podem ser processados em estações de trabalho remotas. Este processo garante que nenhum dado se perca se a conexão de rede falhar durante a aquisição.

O desempenho do sistema pode ficar mais lento quando os projetos em rede estiverem sendo usados do que quando os projetos locais estiverem sendo usados. Como alguns rastreamentos de auditoria também estão nas pastas da rede, qualquer atividade que crie um registro de auditoria de projeto também fica mais lenta. Os arquivos da rede podem levar algum tempo para abrir, dependendo do desempenho da rede. O desempenho da rede não está relacionado somente ao hardware da rede, mas também ao tráfego e design da rede.

Nota: Se o serviço ClearCore2 for interrompido durante a aquisição de rede, os dados parciais da amostra em aquisição no momento da interrupção não serão gravados no arquivo de dados.

Nota: Ao usar a aquisição de rede em um ambiente regulado, sincronize a hora do computador local com o do servidor para obter horários precisos. O horário do servidor é usado para o horário de criação do arquivo. O Gerente de Rastreamento de Auditoria registra o horário de criação do arquivo usando o horário do computador local.

CUIDADO: Potencial perda de dados. Não salve os dados de computadores de múltipla aquisição no mesmo arquivo de dados da rede.

Benefícios do uso da aquisição de rede

A aquisição de dados de rede oferece um método seguro de trabalho com pastas do projeto que residem inteiramente nos servidores de rede. Isso reduz a complexidade envolvida na coleta local de dados e transferência dos dados para um local de rede para armazenamento. Além disso, como o backup dos drives de rede são feitos geralmente de forma automática, a necessidade de backup dos drives locais é reduzida ou eliminada.

Conta de rede segura

Em um ambiente regulado em que os dados estão sendo adquiridos para uma pasta de rede, é altamente recomendado que os usuários normalmente não possuem direitos de exclusão para a pasta de destino. No entanto, sem o acesso de exclusão a essa pasta, o

software SCIEX OS não consegue operar adequadamente. O recursos SNA (secure network account, conta de rede segura) identifica uma conta de rede que possui a permissão de arquivo Full control para o diretório raiz da rede. O serviço ClearCore2 usa essa conta para transferir dados para a pasta de rede.

A SNA deve ter Full control da:

- Pasta do diretório raiz de rede
- Pasta `SCIEX OS Data\NetworkBackup` no computador de aquisição
- Pasta `SCIEX OS Data\TempData` no computador de aquisição

A SNA não precisa:

- Pertencer ao grupo Administrator no computador.
- Estar no banco de dados de gerenciamento de usuários do software SCIEX OS.

A SNA é específica na página Projetos no espaço de trabalho Configuração. Somente uma rede válida do Windows ou conta de domínio pode ser especificada.

Se não for especificada uma SNA, o software SCIEX OS usará as credenciais do usuário conectado no momento para transferir os dados para o diretório raiz da rede. Para que a transferência seja bem-sucedida, a conta deve ter permissões de gravação para todas as pastas do projeto para as quais os dados estão sendo adquiridos, independentemente de qual usuário enviou o lote para aquisição.

Processo de transferência

Quando o software SCIEX OS adquire dados para um local da rede, ele primeiro grava cada amostra em uma pasta da unidade local e, em seguida, transfere-a para a rede. Quando a transferência bem-sucedida de todo o arquivo de dados é confirmado, a pasta local contendo os dados é excluída. Se a rede fica indisponível durante esse processo, o software SCIEX OS tenta novamente a cada 15 minutos até a transferência ser bem-sucedida.

Para obter informações sobre o acesso aos dados durante períodos estendidos de perda de conectividade de rede, consulte a seção: Remover amostras das pastas de transferência de rede.

Configurar aquisição de rede

Um diretório raiz é a pasta em que o software SCIEX OS armazena dados. Para ter certeza de que as informações do projeto estão armazenadas de forma segura, crie o diretório raiz com o software SCIEX OS. Não crie projetos no File Explorer.

Opcionalmente, ao criar os diretórios raízes em um recurso de rede, defina as **Credenciais para conta de rede segura**. Essa é a conta de rede segura definida no recurso de rede. Consulte a seção: Conta de rede segura.

Para obter informações sobre criação de projetos e subprojetos, consulte o documento: *SCIEX OSGuia de usuário do software*.

Especifique uma Conta de rede segura

Se os projetos forem armazenados em um recurso de rede, uma SNA poderá ser especificada, para certificar-se de que todos os usuários da estação de trabalho possuem o acesso exigido ao recurso da rede.

1. Abra o espaço de trabalho de Configuração.
2. Clique em **Projetos**.
3. Na seção **Avançado**, clique em **Credenciais para conta de rede segura**.
4. Digite o nome de usuário, senha e domínio da conta da rede segura definida no recurso da rede.
5. Clique em **OK**.

Auditoria 7

Esta seção explica como usar a funcionalidade de auditoria. Para obter mais informações sobre as funções de auditoria do Windows, consulte a seção: Auditorias do sistema.

Rastreamentos de auditoria

O software organiza os eventos de auditoria no espaço de trabalho Rastreamento de auditoria. O software armazena os eventos de projeto em rastreamentos de auditoria, que são arquivos que armazenam registros dos eventos auditados.

Eventos da estação de trabalho são armazenados na estação de trabalho de rastreamento de auditoria. Os rastreamentos de auditoria da estação de trabalho são arquivos que armazenam os eventos auditados para o computador em que o software SCIEX OS está instalado.

Os eventos do sistema CAC são armazenados nos rastreamentos de auditoria do CAC.

Eventos do projeto são armazenados no rastreamento de auditoria do projeto. O espaço de trabalho Rastreamento de auditoria mostra os rastreamentos de auditoria dos projetos no diretório raiz ativo. Os eventos do processamento de rastreamentos de auditoria estão contidos nos rastreamentos de auditoria do projeto e armazenados com a tabela de resultados.

Para obter uma lista completa de eventos auditados, consulte a seção: Eventos de auditoria.

Os rastreamentos de auditoria, combinados com arquivos como `wiff2` e os da tabela de resultados, são registros eletrônicos válidos que podem ser usados para fins de conformidade.

Tabela 7-1: Rastreamentos de auditoria

Rastreamento de auditoria	Exemplos de eventos registrados	Mapas de auditoria disponíveis armazenados	Mapas de auditoria padrão

Estação de trabalho (SCIEX OS)	• Muda para:
	  • Atribuição do mapa de auditoria ativo
	  • Ajuste do instrumento
	  • Amostras em espera
	  • Segurança
	  • Ajuste
	  • Dispositivos
		• Pasta `C:\ProgramData\SCIEX\Audit Data`	• Sem mapa de auditoria

CAC	• Muda para:
	  • Mapa de auditoria
	  • CAC
	  • Segurança
	  • Log do usuário
		• Pasta `C:\ProgramData\SCIEX\Audit Data`	• Mapa de auditoria silencioso

Projeto (um por projeto)	• Muda para:
	  • Atribuição do mapa de auditoria ativo (SCIEX OS)
	  • Projeto
	  • Dados
	• Impressão
		• Pasta `<project>\Audit Data`	• Especificado na página Mapas de auditoria da estação de trabalho Configuração

Depois que o rastreamento de auditoria contiver 20.000 registros de auditoria, o SCIEX OS e o software CAC arquivarão automaticamente os registros e iniciarão um novo rastreamento de auditoria. Para obter mais informações, consulte a seção: Arquivos de rastreamento de auditoria.

Mapas de auditoria

Um mapa de auditoria é um arquivo que contém uma lista de todos os eventos que podem ser auditados e se uma razão para mudança ou assinatura eletrônica for necessária para o evento. No software SCIEX OS, dois tipos de mapa de auditoria estão disponíveis: estação de trabalho e projeto. Na janela do software CAC, dois tipos de mapa de auditoria estão disponíveis: CAC e projeto.

Os mapas de auditoria controlam os eventos auditados em uma estação de trabalho.

Os mapas de auditoria de projeto controlam os eventos auditados para um projeto e são armazenados na pasta do projeto.

Nota: O mapa de auditoria de um projeto pode ser editado no software SCIEX OS ou Central Administrator Console (CAC).

O usuário pode criar vários mapas de auditoria, mas somente um mapa de auditoria pode ser usado por vez para cada estação de trabalho, sistema CAC e cada projeto. O mapa de auditoria que está sendo usado em um sistema CAC, estação de trabalho ou projeto é chamado de mapa de auditoria ativo.

Quando o software SCIEX OS é instalado, o mapa de auditoria padrão para todos os novos projetos é Sem mapa de auditoria. Quando o software CAC é instalado, o mapa de auditoria padrão para todos os novos projetos é Silent Audit Map. O usuário pode identificar um mapa de auditoria ativo diferente para ser usado como padrão para todos os novos projetos. Consulte a seção: Alteração do mapa de auditoria ativo de um projeto.

Configurar mapas de auditoria

Antes de trabalhar com projetos que necessitam de auditoria, configure mapas de auditoria que sejam apropriados para os procedimentos operacionais padrão. Vários modelos de mapas de auditoria padrão são disponibilizados quando o software é instalado, mas talvez seja necessário criar um mapa personalizado. Certifique-se de que um mapa de auditoria esteja disponível para o rastreamento de auditoria da estação de trabalho ou do CAC e de que um mapa de auditoria esteja disponível para cada projeto.

Tabela 7-2: Lista de verificação para Configuração de auditoria

Tarefa	Consulte

• SCIEX OS: criar um mapa de auditoria para o rastreamento de auditoria da estação de trabalho.
• Software CAC: criar um mapa de auditoria para o rastreamento de auditoria do CAC.
	• SCIEX OS:
	  • Criação de um mapa de auditoria de estações de trabalho
	  • Editar um mapa de auditoria de estações de trabalho
	• Software CAC:
	  • Criar um mapa de auditoria do CAC
	  • Editar um mapa de auditoria do CAC

• SCIEX OS: aplicar o mapa de auditoria ao rastreamento de auditoria da estação de trabalho. • Software CAC: aplicar o mapa de auditoria ao rastreamento de auditoria do CAC.	• SCIEX OS: Alteração do mapa de auditoria ativo de uma estação de trabalho • Software CAC: Alterar o mapa de auditoria ativa para um sistema CAC
Criar um mapa de auditoria ativo padrão para novos projetos.	• Criação de um mapa de auditoria de projetos.
Configurar o mapa de auditoria a ser usado para cada projeto existente.	• Criação de um mapa de auditoria de projetos. • Edição de um mapa de auditoria de projetos.
Aplicar um mapa de auditoria a cada projeto existente.	• Alteração do mapa de auditoria ativo de um projeto.

Modelos de mapas de auditoria instalados

Vários modelos de mapa de auditoria estão incluídos no software. Esses modelos não podem ser editados nem excluídos.

Tabela 7-3: Mapas de auditoria instalados

Mapa de auditoria	Descrição
Exemplo de mapa de auditoria	Os eventos selecionados são auditados. Apenas para fins ilustrativos.

Tabela 7-3: Mapas de auditoria instalados (continuação)

Mapa de auditoria	Descrição
Mapa de auditoria completo	Todos os eventos são auditados. Assinaturas eletrônicas e motivos são requeridos para todos os eventos.
Sem mapa de auditoria	Nenhum evento é auditado. **Nota:** O evento **Alterar atribuição do mapa de auditoria ativo** é sempre registrado, mesmo que seja usado o modelo No Audit Map.
Mapa de auditoria silencioso	Todos os eventos são auditados. Assinaturas eletrônicas e motivos não são obrigatórios para os eventos.

Para descrições dos tipos de rastreamentos de auditoria e sua relação com os mapas de auditoria, consulte a tabela: Tabela 7-1. Para obter informações sobre os eventos registrados em rastreamentos de auditoria, consulte a seção: SCIEX OS Registros de rastreamento de auditoria.

Para obter informações sobre o processo de auditoria, consulte a tabela: Tabela 7-2.

Trabalhar com mapas de auditoria

O software inclui vários modelos de mapa de auditoria instalados. Para obter descrições dos modelos de mapa de auditoria, consulte a seção: Modelos de mapas de auditoria instalados. Para obter uma lista de verificação de passos sugeridos para configurar uma auditoria, consulte a seção: Configurar mapas de auditoria.

Se um modelo de mapa de auditoria ativo for excluído do software ou do File Explorer, o projeto que usa esse modelo de mapa de auditoria usará o mapa de auditoria silencioso.

Mapas de auditoria de projeto

Os mapas de auditoria de projeto controlam a auditoria de eventos de projeto. Para obter uma lista de eventos de projeto auditáveis, consulte a seção: Rastreamento de auditoria do projeto.

Criação de um mapa de auditoria de projetos

1. Abra o espaço de trabalho de Configuração.
2. Clique em **Mapas de auditoria**.
3. Abra a guia Modelos de projetos.
4. No campo **Editar modelo de mapa**, selecione um modelo a ser usado como base para o novo mapa.

5. Clique em **Adicionar modelo** ().
   A caixa de diálogo Adicionar um modelo de mapa de auditoria do projeto é aberta.
6. Insira o nome do novo mapa e, em seguida, clique em **OK**.
7. Selecione e configure os eventos a serem registrados seguindo as etapas a seguir:
   a. Marque a caixa de seleção **Auditado** para o evento.
   b. (Opcional) Se um motivo for exigido, selecione **Motivo necessário**.
   c. (Opcional) Se uma assinatura eletrônica for exigida, selecione **Assinatura eletrônica necessária**.
   d. (Opcional) Se forem exigidos motivos pré-definidos, selecione **Usar somente motivo predefinido** e defina os motivos.
8. Certifique-se de que a caixa de seleção **Auditado** está desmarcada para qualquer evento que não será auditado.
9. Clique em **Salvar modelo**.
   O sistema solicita ao usuário que aplicar o novo mapa aos projetos.
10. Escolha uma das seguintes opções:
    - Para aplicar o novo mapa aos projetos, clique em **Sim**, selecione os projetos que usarão o novo mapa e, em seguida, clique em **Aplicar**.
    - Se o novo mapa não deve ser aplicado aos projetos existentes, clique em **Não**.
11. (Opcional) Para utilizar este mapa de auditoria como padrão para todos os novos projetos, clique em **Usar como padrão para novos projetos**.

Edição de um mapa de auditoria de projetos

Nota: Os modelos de mapa de auditoria instalados não podem ser editados.

1. Abra o espaço de trabalho de Configuração.
2. Clique em **Mapas de auditoria**.
3. Abra a guia Modelos de projetos.
4. No campo **Editar modelo de mapa**, selecione o mapa a ser modificado.
5. Selecione e configure os eventos a serem registrados seguindo as etapas a seguir:
   a. Marque a caixa de seleção **Auditado** para o evento.
   b. (Opcional) Se um motivo for exigido, selecione **Motivo necessário**.
   c. (Opcional) Se uma assinatura eletrônica for exigida, selecione **Assinatura eletrônica necessária**.
   d. (Opcional) Se forem exigidos motivos pré-definidos, selecione **Usar somente motivo predefinido** e defina os motivos.

6. Certifique-se de que a caixa de seleção **Auditado** está desmarcada para qualquer evento que não será auditado.
7. Clique em **Salvar modelo**.
   O sistema solicita ao usuário que aplicar o novo mapa aos projetos.
8. Escolha uma das seguintes opções:
   - Para aplicar o novo mapa aos projetos, clique em **Sim**, selecione os projetos que usarão o novo mapa e, em seguida, clique em **Aplicar**.
   - Se o novo mapa não deve ser aplicado aos projetos existentes, clique em **Não**.

Alteração do mapa de auditoria ativo de um projeto

Quando um mapa de auditoria é aplicado ao projeto, ele se torna o mapa de auditoria ativo. A configuração de auditoria no mapa de auditoria ativo determina quais eventos são registrados nos rastreamentos de auditoria.

1. Abra o espaço de trabalho de Configuração.
2. Clique em **Mapas de auditoria**.
3. Abra a guia Modelos de projetos.
4. No campo **Editar modelo de mapa**, selecione o mapa de auditoria a ser atribuído ao projeto.
5. Clique em **Aplicar aos projetos existentes**.
   A caixa de diálogo Aplicar modelo de mapa de auditoria do projeto é aberta.
6. Marque as caixas de seleção dos projetos aos quais será aplicado este mapa de auditoria.
7. Clique em **Aplicar**.

Exclusão de um mapa de auditoria de projetos

Nota: Os modelos de mapa de auditoria instalados não podem ser excluídos.

1. Abra o espaço de trabalho de Configuração.
2. Clique em **Mapas de auditoria**.
3. Abra a guia Modelos de projetos.
4. No campo **Editar modelo de mapa**, selecione o mapa a ser excluído.
5. Clique em **Excluir modelo**.
   O sistema pede confirmação.
6. Clique em **Sim**.

Mapas de auditoria da estação de trabalho

Os mapas de auditoria da estação de trabalho controlam a auditoria de eventos da estação de trabalho. Para obter uma lista de eventos da estação de trabalho auditáveis, consulte a seção: Rastreamento de auditoria da estação de trabalho.

Criação de um mapa de auditoria de estações de trabalho

1. Abra o espaço de trabalho de Configuração.
2. Clique em **Mapas de auditoria**.
3. Clique na guia Modelos de estação de trabalho.
4. No campo **Editar modelo de mapa**, selecione um modelo a ser usado como base para o novo mapa.
5. Clique em **Adicionar modelo** ().
   A caixa de diálogo Adicionar um modelo de mapa de auditoria da estação de trabalho é aberta.
6. Insira o nome do novo mapa e, em seguida, clique em **OK**.
7. Selecione e configure os eventos a serem registrados seguindo as etapas a seguir:
   a. Marque a caixa de seleção **Auditado** para o evento.
   b. (Opcional) Se um motivo for exigido, selecione **Motivo necessário**.
   c. (Opcional) Se uma assinatura eletrônica for exigida, selecione **Assinatura eletrônica necessária**.
   d. (Opcional) Se forem exigidos motivos pré-definidos, selecione **Usar somente motivo predefinido** e defina os motivos.
8. Certifique-se de que a caixa de seleção **Auditado** está desmarcada para qualquer evento que não será auditado.
9. Clique em **Salvar modelo**.
10. (Opcional) Para tornar este mapa de auditoria o mapa de auditoria ativo para a estação de trabalho, clique em **Aplicar à estação de trabalho**.

Editar um mapa de auditoria de estações de trabalho

Nota: Os modelos de mapa de auditoria instalados não podem ser editados.

1. Abra o espaço de trabalho de Configuração.
2. Clique em **Mapas de auditoria**.
3. Clique na guia Modelos de estação de trabalho.
4. No campo **Editar modelo de mapa**, selecione o mapa a ser alterado.
5. Selecione e configure os eventos a serem registrados seguindo as etapas a seguir:
   a. Marque a caixa de seleção **Auditado** para o evento.
   b. (Opcional) Se um motivo for exigido, selecione **Motivo necessário**.
   c. (Opcional) Se uma assinatura eletrônica for exigida, selecione **Assinatura eletrônica necessária**.

d. (Opcional) Se forem exigidos motivos pré-definidos, selecione **Usar somente motivo predefinido** e defina os motivos.

6. Certifique-se de que a caixa de seleção **Auditado** está desmarcada para qualquer evento que não será auditado.
7. Clique em **Salvar modelo**.
8. (Opcional) Para tornar este mapa de auditoria o mapa de auditoria ativo para a estação de trabalho, clique em **Aplicar à estação de trabalho**.

Alteração do mapa de auditoria ativo de uma estação de trabalho

Quando um mapa de auditoria é aplicado à estação de trabalho, ele se torna o mapa de auditoria ativo. A configuração de auditoria no mapa de auditoria ativo determina quais eventos são registrados nos rastreamentos de auditoria.

1. Abra o espaço de trabalho de Configuração.
2. Clique em **Mapas de auditoria**.
3. Clique na guia Modelos de estação de trabalho.
4. No campo **Editar modelo de mapa**, selecione o mapa a ser aplicado à estação de trabalho.
5. Clique em **Aplicar à estação de trabalho**.

Exclusão de um mapa de auditoria de estações de trabalho

Nota: Os modelos de mapa de auditoria instalados não podem ser excluídos.

1. Abra o espaço de trabalho de Configuração.
2. Clique em **Mapas de auditoria**.
3. Clique na guia Modelos de estação de trabalho.
4. No campo **Editar modelo de mapa**, selecione o mapa a ser excluído.
5. Clique em **Excluir modelo**.
   O sistema pede confirmação.
6. Clique em **Sim**.

Mapas de auditoria do CAC

Os mapas de auditoria do CAC controlam a auditoria de eventos da estação de trabalho do CAC. Para obter uma lista de eventos auditáveis, consulte a seção: Rastreamento de auditoria da estação de trabalho.

Criar um mapa de auditoria do CAC

1. Abra o espaço de trabalho de Configuração.
2. Clique em **Mapas de auditoria**.
3. Clique na guia Modelos do CAC.

4. No campo **Editar modelo de mapa**, selecione um modelo a ser usado como base para o novo mapa.
5. Clique em **Adicionar modelo** ().
   A caixa de diálogo Adicionar um modelo de mapa de auditoria do CAC é aberta.
6. Insira o nome do novo mapa e, em seguida, clique em **OK**.
7. Selecione e configure os eventos a serem registrados seguindo as etapas a seguir:
   a. Marque a caixa de seleção **Auditado** para o evento.
   b. (Opcional) Se um motivo for exigido, selecione **Motivo necessário**.
   c. (Opcional) Se uma assinatura eletrônica for exigida, selecione **Assinatura eletrônica necessária**.
   d. (Opcional) Se forem exigidos motivos pré-definidos, selecione **Usar somente motivo predefinido** e defina os motivos.
8. Certifique-se de que a caixa de seleção **Auditado** está desmarcada para qualquer evento que não será auditado.
9. Clique em **Salvar modelo**.
10. (Opcional) Para tornar este mapa de auditoria o mapa de auditoria ativo da estação de trabalho do CAC, clique em **Aplicar ao CAC**.

Editar um mapa de auditoria do CAC

Nota: Os modelos de mapa de auditoria instalados não podem ser editados.

1. Abra o espaço de trabalho de Configuração.
2. Clique em **Mapas de auditoria**.
3. Clique na guia Modelos do CAC.
4. No campo **Editar modelo de mapa**, selecione o mapa a ser alterado.
5. Selecione e configure os eventos a serem registrados seguindo as etapas a seguir:
   a. Marque a caixa de seleção **Auditado** para o evento.
   b. (Opcional) Se um motivo for exigido, selecione **Motivo necessário**.
   c. (Opcional) Se uma assinatura eletrônica for exigida, selecione **Assinatura eletrônica necessária**.
   d. (Opcional) Se forem exigidos motivos pré-definidos, selecione **Usar somente motivo predefinido** e defina os motivos.
6. Certifique-se de que a caixa de seleção **Auditado** está desmarcada para qualquer evento que não será auditado.
7. Clique em **Salvar modelo**.

8. (Opcional) Para tornar este mapa de auditoria o mapa de auditoria ativo da estação de trabalho do CAC, clique em **Aplicar ao CAC**.

Alterar o mapa de auditoria ativa para um sistema CAC

Quando um mapa de auditoria é aplicado à estação de trabalho do CAC, ele se torna o mapa de auditoria ativo. A configuração de auditoria no mapa de auditoria ativo determina quais eventos são registrados nos rastreamentos de auditoria.

1. Abra o espaço de trabalho de Configuração.
2. Clique em **Mapas de auditoria**.
3. Clique na guia Modelos do CAC.
4. No campo **Editar modelo de mapa**, selecione o mapa a ser aplicado à estação de trabalho.CAC
5. Clique em **Aplicar ao CAC**.

Excluir um mapa de auditoria do CAC

Nota: Os modelos de mapa de auditoria instalados não podem ser excluídos.

1. Abra o espaço de trabalho de Configuração.
2. Clique em **Mapas de auditoria**.
3. Clique na guia Modelos do CAC.
4. No campo **Editar modelo de mapa**, selecione o mapa a ser excluído.
5. Clique em **Excluir modelo**.
   O sistema pede confirmação.
6. Clique em **Sim**.

Visualizar, pesquisar, exportar e imprimir rastreamentos de auditoria

Esta seção fornece informações sobre como visualizar rastreamentos de auditoria arquivados ou não. Oferece também instruções para exportação, impressão, pesquisa e classificação de registros de auditoria em rastreamentos de auditoria.

Visualizar registros de rastreamento de auditoria

1. Abra o espaço de trabalho de Rastreamento de auditoria.
2. No painel esquerdo, clique no rastreamento de auditoria a ser visualizado.
3. Para ver informações detalhadas sobre um evento de auditoria, clique no evento.
   O tipo de evento selecionado controla as informações mostradas. As informações são mostradas em uma ou mais das seguintes guias:

Tabela 7-4: Guias de detalhe do evento

Guia	Informações
Detalhes gerais	Mostra informações como diferença de fuso horário e nome da estação de trabalho.
Antes da mudança	Mostra o conteúdo antes da alteração feita.
Após a mudança	Mostra o conteúdo depois da alteração feita.
Alterar detalhes	Mostra o conteúdo original e o novo conteúdo no mesmo painel. Em Visualização de diferença, o conteúdo original é mostrado em vermelho e o novo conteúdo é mostrado em verde. Em Visualização lado a lado, o conteúdo original e o novo são mostrados em painéis separados para que o usuário possa ver facilmente as alterações.

Buscar ou filtrar registros de auditoria

1. Abra o espaço de trabalho de Rastreamento de auditoria.
2. Selecione o rastreamento de auditoria a ser pesquisado.
3. Para pesquisar um registro de auditoria específico, insira o texto no campo **Buscar na página**.
   Todas as ocorrências de texto especificado na página são realçadas.
4. Para filtrar os registros de rastreamentos de auditoria, siga estas etapas:
   a. Clique no ícone de filtro (funil).
      A caixa de diálogo Filtrar rastreamentos de auditoria é aberta.
   b. Insira os critérios do filtro.
   c. Clique em **OK**.

Visualizar um rastreamento de auditoria arquivado

Depois que o rastreamento de auditoria contiver 20.000 registros de auditoria, o software SCIEX OS arquivará automaticamente os registros e iniciará um novo rastreamento de auditoria. Os arquivos de rastreamento de auditoria arquivados são nomeados com o tipo de rastreamento de auditoria, a data e o horário. Por exemplo, o nome do arquivo de um rastreamento de auditoria de estação de trabalho tem o formato `WorkstationAuditTrailData-<workstation name>>-<YYYY><MMDDHHMMSS>.atds`.

Esse procedimento também pode ser usado para abrir um rastreamento de auditoria para uma Tabela de resultados.

1. Abra o espaço de trabalho de Rastreamento de auditoria.
2. Clique em **Navegar**.

3. Procure e selecione o rastreamento de auditoria arquivado a ser aberto e, em seguida, clique em **OK**.

   Nota: Para abrir o rastreamento de auditoria para uma tabela de resultados, selecione o arquivo `qsession` associado.

Imprimir um Rastreamento de auditoria

1. Abra o espaço de trabalho de Rastreamento de auditoria.
2. Selecione o rastreamento de auditoria a ser impresso.
3. Clique em **Imprimir**.
   A caixa de diálogo Imprimir é aberta.
4. Selecione a impressora e, em seguida, clique em **OK**.

Exportação de registros de rastreamento de auditoria

1. Abra o espaço de trabalho de Rastreamento de auditoria.
2. Selecione o rastreamento de auditoria a ser exportado.
3. Clique em **Exportar**.
4. Navegue até o local em que o arquivo exportado será armazenado, insira um **Nome do arquivo** e, em seguida, clique em **Salvar**.
   O rastreamento de auditoria é salvo como um arquivo csv (valores separados por vírgulas).

SCIEX OS Registros de rastreamento de auditoria

Esta seção descreve os campos nos registros de rastreamento de auditoria.

Os rastreamentos de auditoria da estação de trabalho e do projeto são arquivos criptografados.

Nota: Os rastreamentos de auditoria e arquivos da estação de trabalho são armazenados na pasta `Program Data\SCIEX\Audit Data`. Os rastreamentos de auditoria do projeto e arquivos são armazenados na pasta `Audit Data` do projeto.

Tabela 7-5: Campos de registro de auditoria

Rótulo	Descrição
Carimbo de data e hora	A data e hora em que o registro foi criado.
Nome do evento	O nome do evento.
Descrição	A descrição do evento.
Motivo	O motivo dado para o evento.

Tabela 7-5: Campos de registro de auditoria (continuação)

Rótulo	Descrição
Assinatura eletrônica	Se uma assinatura eletrônica foi inserida para o evento.
Nome completo do usuário	Nome completo do usuário. **Nota:** Para eventos acionados por uma regra de decisão, este é o usuário que enviou o lote.
Usuário	O ID do usuário que iniciou o evento que produziu o registro.
Categoria	A função ou categoria à qual o evento pertence.

O painel inferior do espaço de trabalho Rastreamento de auditoria apresenta informações detalhadas sobre um evento selecionado, inclusive detalhes de alterações, se aplicáveis.

Para listas de todos os eventos que são gravados na estação de trabalho e nos rastreamentos de auditoria de projetos, consulte as seções: Rastreamento de auditoria da estação de trabalho e Rastreamento de auditoria do projeto.

Registros de rastreamento de auditoria do CAC

Esta seção descreve os campos nos registros de rastreamento de auditoria.

Os rastreamentos de auditoria do projeto e do CAC são arquivos criptografados.

Nota: Os rastreamentos de auditoria e arquivos do CAC são armazenados na pasta `Program Data\SCIEX\Audit Data`. Os rastreamentos de auditoria do projeto e arquivos são armazenados na pasta `Audit Data` do projeto.

Tabela 7-6: Campos de registro de auditoria

Rótulo	Descrição
Carimbo de data e hora	A data e hora em que o registro foi criado.
Nome do evento	O nome do evento.
Descrição	A descrição do evento.
Motivo	O motivo dado para o evento.
Assinatura eletrônica	Se uma assinatura eletrônica foi inserida para o evento.
Nome completo do usuário	Nome completo do usuário. **Nota:** Para eventos acionados por uma regra de decisão, este é o usuário que enviou o lote.

Tabela 7-6: Campos de registro de auditoria (continuação)

Rótulo	Descrição
Usuário	O ID do usuário que iniciou o evento que produziu o registro.
Categoria	A função ou categoria à qual o evento pertence.

O painel inferior do espaço de trabalho Rastreamento de auditoria apresenta informações detalhadas sobre um evento selecionado, inclusive detalhes de alterações, se aplicáveis.

Para ver as listas de todos os eventos gravados no CAC e nos rastreamentos de auditoria de projetos, consulte as seções: Tabela 3 e Rastreamento de auditoria do projeto.

Arquivos de rastreamento de auditoria

Os registros de auditoria se acumulam no rastreamento de auditoria do projeto e rastreamento de auditoria do da estação de trabalho e podem criar arquivos grandes que são difíceis de navegar e gerenciar.

Quando um rastreamento de auditoria atinge 20.000 registros, ele é arquivado. Um registro final para arquivo é adicionado ao rastreamento de auditoria e, em seguida, o registro de auditoria é salvo com um nome que indica o tipo de rastreamento de auditoria, a data e a hora. Um novo rastreamento de auditoria é criado. O primeiro registro no novo rastreamento de auditoria afirma que o rastreamento de auditoria foi arquivado e especifica o caminho até o rastreamento de auditoria arquivado.

Os arquivos de rastreamento de auditoria de estação de trabalho são armazenados na pasta `C:\ProgramData\SCIEX\Audit Data`. Os nomes dos arquivos estão no formato WorkstationAuditTrailData-*<nome da estação de trabalho>*-*<AAAA><MMDDHHMMSS>*.atds. Por exemplo, `WorkstationAuditTrailData-SWDSXPT158-20190101130401.atds`.

Os arquivos de rastreamento de auditoria de projetos são armazenados na pasta `Audit Data` do projeto.

Acessar dados durante falha na rede A

Visualizar e processar dados localmente

Se um distúrbio temporário da rede ocorrer durante a aquisição da rede, os dados adquiridos podem ser acessados na pasta `NetworkBackup` no computador de aquisição. Para evitar corrupção dos dados, recomendamos que os arquivos de dados na pasta `NetworkBackup` sejam copiados para uma nova localização antes de serem visualizados ou processados e que a cópia original dos arquivos seja mantida na pasta `NetworkBackup`.

A cada 15 minutos, o software SCIEX OS determina se a localização da rede está disponível. Se estiver, a transferência de dados é retomada.

A pasta `NetworkBackup` é armazenada no diretório raiz local, normalmente `D:\SCIEX OS Data\NetworkBackup`. Os arquivos de dados para cada lote são armazenados em uma pasta com um identificador específico como o nome da pasta. Os carimbos de data e hora das pastas mostram a data e hora inicial do lote, e eles podem ser usados para determinar que pasta contém os dados de interesse.

Remover amostras das pastas de transferência de rede

Se a conectividade da rede for perdida por um período ampliado, ou se o diretório raiz da rede for alterado, pode ser necessário remover arquivos de dados das pastas de transferência de rede. Recomendamos que esta ação seja realizada por um administrador do sistema com um alto nível de habilidade técnica da rede.

1. Abra o espaço de trabalho do Fila.
2. Parar a fila.
3. Cancele todas as amostras restantes no lote que contém as amostras a serem removidas.
4. Feche o software SCIEX OS.
5. Parar **Clearcore2.Service.exe**.

   Dica! Realize esta tarefa no Windows Services Manager.

6. Mova todos os arquivos e pastas das pastas `OutBox` e `NetworkBackup` que estão aguardando a transferência para o diretório raiz indisponível para outra pasta temporariamente. Não exclua as pastas `OutBox` ou `NetworkBackup`.

Nota: A pasta `OutBox` é uma pasta oculta no diretório raiz local, normalmente `D:\SCIEX OS Data\TempData\Outbox`. Quando os arquivos e pastas no `Outbox` não são mais necessários, eles podem ser removidos.

CUIDADO: Potencial perda de dados. Não exclua o arquivo se os dados na amostra retida devem ser preservados.

7. Abra o software SCIEX OS.
   Em 15 minutos, o software SCIEX OS tenta conectar-se ao recurso da rede. Se a conexão for bem-sucedida, a transferência é retomada. Quando a transferência é concluída, as pastas da pasta `NetworkBackup` são excluídas.

Permissões do Windows B

Esta seção fornece uma lista de permissões do Windows necessárias a cada função de usuário e ao usuário SYSTEM para a correta operação do software SCIEX OS.

Nota: O caminho padrão da pasta *Installed Root Directory* é `D:\SCIEX OS Data`.

Tabela B-1: *Pasta* Installed Root Directory

Privilégio	Administrador, SYSTEM	Analista, desenvolvedor de métodos, revisor
Controle total	Permitir	—
Percorrer pasta / Executar arquivo	Permitir	Permitir
Listar pastas / Ler dados	Permitir	Permitir
Ler atributos	Permitir	Permitir
Ler atributos estendidos	Permitir	Permitir
Criar arquivos / Gravar dados	Permitir	Permitir
Criar pastas / Anexar dados	Permitir	Permitir
Gravar atributos	Permitir	Permitir
Gravar atributos estendidos	Permitir	Permitir
Excluir subpastas e arquivos	Permitir	—
Excluir	Permitir	—
Ler permissões	Permitir	Permitir
Alterar permissões	Permitir	—
Apropriar-se	Permitir	—

Tabela B-2: Pastas *Installed Root Directory*\NetworkBackup e *Installed Root Directory*\TempData

Privilégio	Administrador, SYSTEM	Analista, desenvolvedor de métodos, revisor
Controle total	Permitir	—
Percorrer pasta / Executar arquivo	Permitir	Permitir
Listar pastas / Ler dados	Permitir	Permitir
Ler atributos	Permitir	Permitir
Ler atributos estendidos	Permitir	Permitir
Criar arquivos / Gravar dados	Permitir	Permitir
Criar pastas / Anexar dados	Permitir	Permitir
Gravar atributos	Permitir	Permitir
Gravar atributos estendidos	Permitir	Permitir
Excluir subpastas e arquivos	Permitir	Permitir
Excluir	Permitir	Permitir
Ler permissões	Permitir	Permitir
Alterar permissões	Permitir	—
Apropriar-se	Permitir	—

Tabela B-3: Pasta C:\ProgramData\SCIEX\Audit Data

Privilégio	Administrador, SYSTEM	Analista, desenvolvedor de métodos, revisor
Controle total	Permitir	—
Percorrer pasta / Executar arquivo	Permitir	Permitir
Listar pastas / Ler dados	Permitir	Permitir
Ler atributos	Permitir	Permitir

Tabela B-3: Pasta `C:\ProgramData\SCIEX\Audit Data` (continuação)

Privilégio	Administrador, SYSTEM	Analista, desenvolvedor de métodos, revisor
Ler atributos estendidos	Permitir	Permitir
Criar arquivos / Gravar dados	Permitir	Permitir
Criar pastas / Anexar dados	Permitir	Permitir
Gravar atributos	Permitir	Permitir
Gravar atributos estendidos	Permitir	Permitir
Excluir subpastas e arquivos	Permitir	—
Excluir	Permitir	—
Ler permissões	Permitir	Permitir
Alterar permissões	Permitir	—
Apropriar-se	Permitir	—

Eventos de auditoria C

Esta seção lista os eventos de auditoria no SCIEX OS. Ela também lista os eventos de auditoria correspondentes no software Analyst, para usuários que estão migrando do software Analyst para o SCIEX OS.

Rastreamento de auditoria do projeto

Cada projeto tem um rastreamento de auditoria do projeto. Os rastreamentos de auditoria do projeto são armazenados na pasta `Audit Data` do projeto. O nome do arquivo de rastreamentos de auditoria é `ProjectAuditEvents.atds`.

Nota: O mapa de auditoria padrão para novos projetos criados no software Central Administrator Console (CAC) é o Mapa de auditoria silencioso.

Os eventos do rastreamento de auditoria do projeto são exibidos no software CAC e no SCIEX OS.

Tabela C-1: Eventos de rastreamento de auditoria do projeto

SCIEX OS ou CAC	Software Analyst
Espaço de trabalho Analytics	
Concentração real alterada	Eventos de quantificação: **'Concentration' has been changed**
Arquivo de processamento automático salvo	—
ID do código de barras alterado	—
Amostra de comparação alterada no fluxo de trabalho não direcionado	—
Colunas personalizadas modificadas	Eventos de quantificação: **'Custom Title' has changed**
Exploração de dados aberto	Eventos de projeto: **Data File has been opened**
Dados exportados	—
Dados transferidos para LIMS	—
Fator de diluição alterado	Eventos de quantificação: **'Dilution Factor' has been changed**
Calibração externa alterada	—
Calibração externa exportada	—

Tabela C-1: Eventos de rastreamento de auditoria do projeto (continuação)

SCIEX OS ou CAC	Software Analyst
Arquivo salvo	Eventos de projeto: **Quantitation Results Table has been created**, **Quantitation Results Table has been modified**, Eventos de quantificação: **Results Table has been saved**
Coluna de fórmulas alterada	Eventos de quantificação: **Formula name has been changed**, **Formula name has been added**, **Formula string has been changed**, **Formula column has been removed**
Integração apagada	—
Parâmetros de integração alterados	Eventos de quantificação: **Quantitation peak has been integrated**
Resultado da pesquisa na biblioteca alterado	—
Integração manual	Eventos de quantificação: **Quantitation Peak has been integrated**
Integração manual revertida	Eventos de quantificação: **Quantitation peak has been reverted back to original**
Seleção MS/MS alterada	—
Método de processamento alterado e aplicado	Eventos de quantificação: **Quantitation method has been changed**
Método de processamento salvo	—
Configurações padrão do projeto alteradas	—
Relatório criado	Eventos de projeto: **Printing document on printer, Finished printing document on printer**
Tabela de resultados aprovada	Eventos de quantificação: **QA reviewer has accessed a results table**
Tabela de resultados criada	Eventos de quantificação: **Results table has been created**
Tabela de resultados bloqueada	—
Tabela de resultados desbloqueada	—
ID da amostra alterado	Eventos de quantificação: **'Sample ID' has been changed**

Tabela C-1: Eventos de rastreamento de auditoria do projeto (continuação)

SCIEX OS ou CAC	Software Analyst
Nome da amostra alterado	Eventos de quantificação: **'Sample Name' has been changed**
Tipo de amostra alterado	Eventos de quantificação: **'Sample Type' has been changed**
Amostras adicionadas ou removidas	Eventos de quantificação: **Files have been added to Results Table**, **Files have been removed from Results Table**, **Samples have been added/removed**
Padrão de concentração real de adição alterada	—
Seleção da coluna usada alterada	Eventos de quantificação: **'Use IT' has been changed**
Peso/volume alterado	**'Weight to Volume Ratio' has been changed**
Janela/painel impresso	Eventos de projeto: **Printing document on printer**, **Finished printing document on printer**
Mapa de auditoria Página	
Mapa de auditoria do projeto alterado	Eventos de projeto: **Project Settings have been changed**
Rastreamento de auditoria do projeto exportado	—
Rastreamento de auditoria do projeto impresso	—
Espaço de trabalho Lote	
Informações do lote importadas de LIMS/ texto	—
Lote salvo	—
Lote enviado	Eventos de instrumento: **Batch file submitted**
Imprimir	Eventos de projeto: **Printing Document on printer**, **Finished printing document on printer**
Espaço de trabalho Explorador[4]	

[4] Os eventos de Explorador são registrados nos rastreamentos de auditoria do projeto quando os usuários usam dados do projeto ativo.

Tabela C-1: Eventos de rastreamento de auditoria do projeto (continuação)

SCIEX OS ou CAC	Software Analyst
Abrir amostra(s)	Eventos de projeto: **Data File has been opened**
Imprimir	Eventos de projeto: **Printing Document on printer**, **Finished printing document on printer**
Recalibrar amostra(s)	—
Recalibração de amostra(s) iniciada	—
Espaço de trabalho Método de LC	
Método de LC salvo	—
Imprimir	Eventos de projeto: **Printing Document on printer**, **Finished printing document on printer**
Espaço de trabalho Método de MS	
Método de MS salvo	—
Imprimir	Eventos de projeto: **Printing Document on printer**, **Finished printing document on printer**
Espaço de trabalho Fila	
A aquisição de amostras foi concluída	—
Amostra editada	—
A amostra começa a adquirir	—
Amostra transferida	—

Rastreamento de auditoria da estação de trabalho

Cada estação de trabalho tem um único rastreamento de auditoria de estação de trabalho. O rastreamento de auditoria da estação de trabalho é armazenado na pasta `Program Data\SCIEX\Audit Data`. O nome do arquivo do rastreamento de auditoria está no formato: `WorkstationAuditTrailData.atds`.

Nota: O mapa de auditoria padrão para novas estações de trabalho no software Central Administrator Console (CAC) é o **Mapa de auditoria silencioso**.

Os eventos do rastreamento de auditoria são exibidos no software CAC e no SCIEX OS.

Tabela C-2: Eventos do rastreamento de auditoria da estação de trabalho

SCIEX OS	Software Analyst
Mapa de auditoria	
Mapa de auditoria da estação de trabalho de alterado	Eventos de instrumento: **Instrument Settings have been changed**
Rastreamento de auditoria da estação de trabalho impresso	—
Rastreamento de auditoria da estação de trabalho exportado	—
CAC	
Administração central habilitada/ desabilitada	—
Não foi possível recuperar as configurações da Administração central/ Configurações da Administração central recuperadas	—
Soma de verificação de arquivo de dados	
A soma de verificação do arquivo de dados wiff foi alterada	—
Espaço de trabalho Explorador[5]	
Abrir amostra(s)	Eventos de projeto: **Data File has been opened**
Imprimir	Eventos de projeto: **Printing document on printer**, **Finished printing document on printer**
Recalibrar amostra(s)	—
Recalibração de amostra(s) iniciada	—
Configuração de hardware	
Dispositivos ativados	Eventos de instrumento: **Hardware profile has been activated**
Dispositivos desativados	Eventos de instrumento: **Hardware profile has been deactivated**
Ajuste do instrumento	
Atualização de ajuste MS automático	Eventos de instrumento: **Tune parameter settings changed**

[5] Os eventos de Explorador são registrados nos rastreamentos de auditoria da estação de trabalho quando os usuários usam dados que não estão no projeto ativo.

Tabela C-2: Eventos do rastreamento de auditoria da estação de trabalho (continuação)

SCIEX OS	Software Analyst
Firmware alterado	—
Modificações de ajuste MS	Eventos de instrumento: **Tune parameter settings changed**
Imprimir o resultado do procedimento em ajuste MS	Eventos de projeto: **Printing Document on printer**, **Finished printing document on printer**
Espaço de trabalho Fila	
Ocorreu uma injeção automática	—
Ocorreu uma reinjeção automática	—
Lote movido na fila	Eventos de instrumento: **Move Batch**
Fila de impressão	Eventos de projeto: **Printing Document on printer**, **Finished printing document on printer**
Readquirindo amostra	Eventos de instrumento: **Reacquiring sample(s)**
A aquisição de amostras foi concluída	Eventos de projeto: **Sample has been added to Data file**
Amostra editada	—
Amostra movida na fila	Eventos de instrumento: **Sample moved from position *x* to position *y* of Batch File**
A amostra começa a adquirir	—
Segurança	
Logoff automático pelo sistema	Eventos de instrumento: **User Logged out**
Logoff forçado por outro usuário	Eventos de instrumento: **User Logged out**
Logoff forçado malsucedido	—
Desbloqueio de tela malsucedido	—
As credenciais da Conta de rede segura foram modificadas	Eventos de instrumento: **Acquisition Account Changed**
As credenciais da Conta de rede segura foram removidas	Eventos de instrumento: **Acquisition Account Changed**
As credenciais da Conta de rede segura foram especificadas	Eventos de instrumento: **Acquisition Account Changed**

Tabela C-2: Eventos do rastreamento de auditoria da estação de trabalho (continuação)

SCIEX OS	Software Analyst
Configuração de segurança alterada	Eventos de instrumento: **The Security Configuration has been modified**, **Screen Lock Changed**, **Auto Logout changed**
Usuário adicionado/excluído	Eventos de instrumento: **User Added**, **User Deleted**
O usuário está conectado	Eventos de instrumento: **User Logged In**
O usuário encerrou a sessão	Eventos de instrumento: **User Logged out**
O usuário desativou o modo exclusivo	—
Login de usuário malsucedido	Eventos de instrumento: **User Login Failed**
As configurações de gerenciamento do usuário foram exportadas	—
As configurações de gerenciamento do usuário foram importadas	—
As configurações de gerenciamento do usuário foram restauradas	—
Função do usuário atribuída ao usuário/ grupo de usuários	Eventos de instrumento: **User Changed User Type**
Função do usuário excluída	Eventos de instrumento: **User Type Deleted**
Função do usuário modificada	Eventos de instrumento: **User Type Changed**
UserLog	
Imprimir log de eventos	—

Tabela C-3: Eventos do rastreamento de auditoria do CAC

CAC	Software Analyst
Página Mapa de auditoria	
Mapa de auditoria da estação de trabalho de alterado	Eventos de instrumento: **Instrument Settings have been changed**
Rastreamento de auditoria da estação de trabalho impresso	—
Rastreamento de auditoria da estação de trabalho exportado	—
CAC	

Tabela C-3: Eventos do rastreamento de auditoria do CAC (continuação)

CAC	Software Analyst
As configurações de CAC foram exportadas	—
As configurações de CAC foram importadas	—
As configurações de CAC foram restauradas	—
Configurações do projeto habilitadas/ desabilitadas em um grupo de trabalho	—
Projeto atribuído/não atribuído a um grupo de trabalho	—
Permissão de segurança adicionada para a administração central	—
Usuário adicionado/excluído	—
Função do usuário adicionada	—
Função do usuário excluída	—
Função do usuário modificada	—
Função(ões) do usuário atribuídas/com atribuição desfeita para usuário(s) no grupo de trabalho	—
Usuário(s)/Grupo(s) de usuários atribuídos/com atribuição desfeita a um grupo de trabalho	—
Grupo de trabalho adicionado/excluído	—
Grupo de trabalho renomeado	—
Estações de trabalho atribuídas/com atribuição desfeita a um grupo de trabalho	—
Segurança	
Logoff automático pelo sistema	Eventos de instrumento: **User Logged out**
Logoff forçado por outro usuário	Eventos de instrumento: **User Logged out**
Logoff forçado malsucedido	—
Desbloqueio de tela malsucedido	—
As credenciais da Conta de rede segura foram modificadas	Eventos de instrumento: **Acquisition Account Changed**

Tabela C-3: Eventos do rastreamento de auditoria do CAC (continuação)

CAC	Software Analyst
As credenciais da Conta de rede segura foram removidas	Eventos de instrumento: **Acquisition Account Changed**
As credenciais da Conta de rede segura foram especificadas	Eventos de instrumento: **Acquisition Account Changed**
Configuração de segurança alterada	Eventos de instrumento: **The Security Configuration has been modified**, **Screen Lock Changed**, **Auto Logout changed**
Usuário adicionado/excluído	Eventos de instrumento: **User Added**, **User Deleted**
O usuário está conectado	Eventos de instrumento: **User Logged In**
O usuário encerrou a sessão	Eventos de instrumento: **User Logged out**
O usuário desativou o modo exclusivo	—
Login de usuário malsucedido	Eventos de instrumento: **User Login Failed**
As configurações de gerenciamento do usuário foram exportadas	—
As configurações de gerenciamento do usuário foram importadas	—
As configurações de gerenciamento do usuário foram restauradas	—
Função do usuário atribuída ao usuário/ grupo de usuários	Eventos de instrumento: **User Changed User Type**
Função do usuário excluída	Eventos de instrumento: **User Type Deleted**
Função do usuário modificada	Eventos de instrumento: **User Type Changed**
UserLog	
Imprimir log de eventos	—

Mapeamento de permissões entre o software SCIEX OS e o Analyst D

Esta seção destina-se a usuários que estão migrando do software Analyst para o SCIEX OS, para ajudá-los a migrar suas configurações de segurança do usuário. Mostra as permissões no software Analyst correspondentes às permissões no software SCIEX OS.

Tabela D-1: Mapeamento de permissões

Software SCIEX OS	Software Analyst
Espaço de trabalho Lote	
Enviar métodos desbloqueados	—
Abrir	Lote: **Open Existing Batches**
Salvar como	Lote: **Create New Batches**, **Import**, **Edit Batches**, **Save Batches**, **Overwrite Batches**
Enviar	Lote: **Submit Batches**
Salvar	Lote: **Save Batches**, **Overwrite Batches**
Saltar tabela de referência de íons	—
Adicionar subpastas de dados	—
Configurar regras de decisão	—
Espaço de trabalho Configuração	
Guia Geral	—
Geral: alterar a configuração regional	—
Geral: modo de tela inteira	—
Geral: interromper serviços do Windows	—
Guia Comunicação LIMS	—
Guia Mapas de auditoria	Gerente de rastreamento de auditoria: **Change Audit Trail Settings**, **Create or Modify Audit Maps**
Guia Fila	—
Fila: tempo de ociosidade do instrumento	—
Fila: número máx. de amostras adquiridas	—
Fila: outras configurações de fila	—

Tabela D-1: Mapeamento de permissões (continuação)

Software SCIEX OS	Software Analyst
Guia Projetos	—
Projetos: criar projeto	Aplicativo Analyst: **Create Project**
Projetos: aplicar um modelo de mapa de auditoria a um projeto existente	Gerente de rastreamento de auditoria: **Change Audit Trail Settings**
Projetos: criar diretório raiz	Aplicativo Analyst: **Create Root Directory**
Projeto: definir diretório raiz atual	Aplicativo Analyst: **Set Root Directory**
Projetos: especificar credenciais da rede	—
Projetos: habilitar a gravação da soma de verificação para criação de dados wiff	—
Projetos: apagar diretório raiz	—
Guia Dispositivos	Configuração de hardware: **Create**, **Delete**, **Edit**, **Activate/Deactivate**
Guia Gerenciamento de usuários	**Security Config**
Forçar logoff do usuário	**Unlock/Logout Application**
Guia CAC[3]	—
Guia Modelos de impressão	—
Modelos de impressão: crie e modifique modelos de impressão	—
Modelos de impressão: defina o modelo de impressão padrão	—
Modelos de impressão: aplique o modelo atual a todos os projetos no diretório raiz	
Espaço de trabalho Registro de eventos	
Acessar espaço de trabalho do registro de eventos	—
Arquivar registro	—
Espaço de trabalho Rastreamento de auditoria	
Acessar espaço de trabalho do rastreamento de auditoria	Gerente de rastreamento de auditoria: **View Audit Trail Data**
Visualizar mapa de auditoria ativo	Gerente de rastreamento de auditoria: **View Audit Trail Data**

[3] Na versão 3.1, a permissão **Habilitar administração central** foi renomeada para **CAC**. A página CAC do espaço de trabalho Configuração pode ser usada para configurar a administração central do software SCIEX OS.

Tabela D-1: Mapeamento de permissões (continuação)

Software SCIEX OS	Software Analyst
Imprimir/Exportar rastreamento de auditoria	Gerente de rastreamento de auditoria: **View Audit Trail Data**
Painel Data Acquisition	
Start (Iniciar)	—
Parar	—
Salvar	—
Espaços de trabalho Método de MS e Método de LC	
Acessar espaço de trabalho Method	—
Novo	Método de aquisição: **Create/Save acquisition method**
Abrir	Método de aquisição: **Open acquisition method as read-only (acquire mode)**
Salvar	Método de aquisição: **Overwrite acquisition methods**, **Create/Save acquisition method**
Salvar como	Método de aquisição: **Overwrite acquisition methods**, **Create/Save acquisition method**
Bloquear/Desbloquear método	—
Espaço de trabalho Fila	
Gerenciar	Fila de amostras: **Reacquire**, **Delete Sample or Batch**, **Move Batch**
Iniciar/Parar	Fila de amostras: **Start Sample**, **Stop Sample**, **Abort Sample**, **Stop Queue**
Imprimir	Editor de modelo de relatório: **Print**
Editar amostra	—
Espaço de trabalho Biblioteca	
Acessar espaço de trabalho Library	Explorar: **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**
Espaço de trabalho Ajuste de MS	
Acessar espaço de trabalho Ajuste MS	—

Tabela D-1: Mapeamento de permissões (continuação)

Software SCIEX OS	Software Analyst
Ajuste MS avançado	Ajuste: **Instrument Optimization**, **Manual Tune**, **Edit Tuning Options**
Resolução de problemas avançada	—
Verificação rápida de status	Ajuste: **Instrument Opt**
Restaurar dados do instrumento	Ajuste: **Edit Tuning Options**, **Edit instrument data**
Espaço de trabalho Explorador	
Acessar espaço de trabalho Explorer	—
Exportar	Explorar: **Save data to text file**
Imprimir	Editor de modelo de relatório: **Print**
Opções	—
Recalibrar	Ajuste: **Calibrate from current spectrum**
Espaço de trabalho Analytics	
Novos resultados	Quantificação: **Create new results tables**
Criar método de processamento	Quantificação: **Create quantitation methods**
Modificar método de processamento	Quantificação: **Modify existing methods**
Permitir a exportação e criar relatório de Tabela de resultados desbloqueada	—
Salvar resultados para o lote de automação	—
Alterar algoritmo de integração de método de quantificação padrão	Quantificação: **Change default method options**
Alterar parâmetros de integração de método de quantificação padrão	Quantificação: **Change default method options**
Habilitar aviso de pico modificado do projeto	—
Adicionar amostras	Quantificação: **Add and Remove samples from results table**
Remover amostras selecionadas	Quantificação: **Add and Remove samples from results table**
Exportar, importar ou remover calibração externa	—
Modificar nome da amostra	Quantificação: **Modify sample name**

Tabela D-1: Mapeamento de permissões (continuação)

Software SCIEX OS	Software Analyst
Modificar tipo da amostra	Quantificação: **Modify Sample Type**
Modificar ID da amostra	Quantificação: **Modify Sample ID**
Modificar concentração real	Quantificação: **Modify Analyte Concentration**
Modificar fator de diluição	Quantificação: **Modify Dilution Factor**
Modificar campos de comentário	Quantificação: **Modify Sample Comment**
Habilitar integração manual	Quantificação: **Manually integrate**
Definir pico como não encontrado	—
Incluir ou excluir um pico da tabela de resultados	Quantificação: **Exclude standards from calibration**
Opções de regressão	Quantificação: **Change regression parameters**
Modificar parâmetros de integração da tabela de resultados para um único cromatograma	Quantificação: **Change "simple" parameters in peak review, Change "advanced" parameters in peak review**
Modificar o método quantitativo para o componente da tabela de resultados	Quantificação: **Edit results tables' method**
Criar novas configurações de gráfico métrico	Quantificação: **Modify or create metric plot settings**
Adicionar colunas personalizadas	Quantificação: **Create or modify formula columns**
Definir formato de título de análise de pico	—
Remover coluna personalizada	Quantificação: **Create or modify formula columns**
Configurações de exibição da Tabela de resultados	Quantificação: **Change results table column precision**, **Change results table column visibility**, **Modify results table settings**
Bloquear tabela de resultados	—
Desbloquear tabela de resultados	—
Marcar arquivo de resultados como revisado e salvar	—
Modificar modelo de relatório	Editor de modelo de relatório: **Create/ Modify report templates**

Tabela D-1: Mapeamento de permissões (continuação)

Software SCIEX OS	Software Analyst
Transferir resultados para o LIMS	—
Modificar coluna do código de barras	—
Alterar atribuição da amostra de comparação	—
Adicionar espectros de MS/MS à biblioteca	Explorar: **Add spectrum to library record**
Configurações padrão do projeto	Quantificação: **Modify global (default) settings**
Criar relatórios em todos os formatos	—
Editar parâmetros dos critérios de alerta	—
Alteração do parâmetro de remoção automática do valor discrepante	—
Habilitar remoção automática do valor discrepante	—
Atualizar método de processamento FF/LS	—
Atualizar resultados via FF/LS	—
Habilitar agrupamento por funcionalidade de adutos	Quantificação: **Create Analyte Groups**, **Modify Analyte Groups**
Buscar arquivos	—
Habilitar adição padrão	—
Definir regra de porcentagem de integração manual	Quantificação: **Enable or Disable percent rule in Manual Integration**
Modificar peso/volume	Quantificação: **Modify Weight To Volume ratio**

Soma de verificação de arquivo de dados E

Recomendamos que os usuários usem as somas de verificação para os arquivos wiff. O recurso de soma de verificação é uma verificação de redundância cíclica para checar a integridade do arquivo de dados.

Se o recurso Soma de verificação do arquivo de dados estiver habilitado, sempre que o usuário criar um arquivo de dados (wiff), o software gera um valor de soma de verificação usando um algoritmo com base no algoritmo de criptografia pública MD5 e salva o valor no arquivo. Quando a soma de verificação é verificada, o software calcula a soma de verificação e compara a soma de verificação calculada com a soma de verificação armazenada no arquivo.

A comparação da soma de verificação pode ter três resultados:

- Se os valores forem correspondentes, a soma de verificação é válida.
- Se os valores não forem correspondentes, a soma de verificação é inválida. Uma soma de verificação inválida indica que o arquivo foi modificado fora do software ou que o arquivo foi salvo quando o cálculo da soma de verificação estava habilitado e a soma de verificação é diferente da soma de verificação original.
- Se o arquivo não tem valor de soma de verificação armazenado, a soma de verificação não é encontrada. Um arquivo não possui valor de soma de verificação armazenado porque o arquivo foi salvo quando o recurso Soma de verificação do arquivo de dados estava desabilitado.

Nota: O usuário pode verificar a soma de verificação usando o software Analyst. Consulte a documentação do software Analyst.

Ativar ou desativar o recurso de soma de verificação do arquivo de dados

1. Abra o espaço de trabalho de Configuração.
2. Clique em **Projetos**.
3. Se necessário, expanda **Segurança do arquivo de dados**.
4. Para habilitar o recursos de soma de verificação do arquivo de dados, marque a caixa de seleção **Habilitar a gravação da soma de verificação para criação de dados wiff**. Para desabilitar o recurso, desmarque essa caixa de seleção.

Entre em contato conosco

Treinamento do consumidor

- Na América do Norte: NA.CustomerTraining@sciex.com
- Na Europa: Europe.CustomerTraining@sciex.com
- Fora da União Europeia e da América do Norte, visite sciex.com/education para obter informações de contato.

Centro de aprendizagem online

- SCIEX Now Learning Hub

Suporte da SCIEX

A SCIEX e seus representantes mantêm uma equipe de atendimento totalmente treinada e especialistas técnicos localizados em todo o mundo. Eles podem responder perguntas sobre o sistema ou quaisquer problemas técnicos que possam surgir. Para obter mais informações, visite o site da SCIEX em sciex.com ou entre em contato conosco através de uma das seguintes maneiras:

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

Segurança cibernética

Para obter informações sobre as orientações mais recentes sobre cibersegurança para produtos da SCIEX, visite sciex.com/productsecurity.

Documentação

Esta versão do documento substitui todas as versões anteriores deste documento.

Para ver este documento eletronicamente é necessário ter o Adobe Acrobat Reader. Para fazer download da versão mais recente, acesse https://get.adobe.com/reader.

Para encontrar a documentação do software, consulte as notas de versão do software ou o guia de instalação do software que o acompanha.

Para encontrar a documentação do produto de hardware, consulte a documentação que acompanha o sistema ou o componente.

As versões mais recentes da documentação estão disponíveis no site da SCIEX, em sciex.com/customer-documents.

Nota: Para solicitar uma versão impressa gratuita, entre em contato com sciex.com/contact-us.