SCIEX
The Power of Precision

Software SCIEX OS

Guia do diretor do laboratório

RUO-IDV-05-7370-PT-I

Junho de 2022

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 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 da instalação do SCIEX OS.

Conformidade regulatória e de segurança

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.

SCIEX OS e Windows Security: trabalhando juntos

O SCIEX OS e o Sistema de arquivos com nova tecnologia (NTFS) do Windows têm recursos de segurança projetados para controlar o acesso ao sistema e 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 de segurança do Windows.

O SCIEX OS possui os seguintes modos de acesso 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 SCIEX OS.

Rastreamentos de auditoria no SCIEX OS e Windows

Os recursos de auditoria do 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 no rastreamento de auditoria incluem a exclusão de funções e a exclusão de usuários do SCIEX OS.
- Criação e modificação das informações da amostra, parâmetros de integração de pico e método de processamento incorporado em uma Tabela de resultados.

Nota: O SCIEX OS não realiza criação de auditoria ou alterações aos métodos de MS, métodos de LC, lotes ou métodos de processamento. Esses arquivos atuam como modelos. Valores de parâmetros são lidos neles no momento da aquisição ou processamento e aplicados à tarefa. Para métodos de MS, métodos de LC e lotes, os valores de parâmetro são registrados nos arquivos wiff e wiff2. Para os métodos de processamento, eles são registrados no arquivo qsession. Esses arquivos servem como registros eletrônicos para essas informações.

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

O 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

SCIEX OS contém os controles técnicos para suportar 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 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 dar suporte à conformidade com a 21 CFR Part 11. O fato de o uso do SCIEX OS estar em conformidade com a 21 CFR Part 11 depende do seu uso real e da configuração do SCIEX OS no laboratório.

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

Nota: Não deixe o software Instrument Parameters Converter em um sistema validado. Destina-se à transferência inicial das configurações do instrumento do software Analyst para SCIEX OS. Certifique-se de remover o software Instrument Parameters 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 de segurança do Windows

O sistema implementa as seguintes restrições para as contas de usuário local 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**, **administrator** ou **demo**.

O administrador do SCIEX OS deve poder alterar as permissões do arquivo 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 ter certeza de que todos os usuários possuem o acesso solicitado aos recursos da aquisição de rede, o administrador da rede pode definir uma Conta de rede segura (SNA) no 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.

Usuários e grupos

O 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 adicionar e configurar pessoas e funções, consulte a seção: Configurar acesso ao SCIEX OS.

Suporte do diretório ativo

Ao adicionar usuários ao espaço de trabalho Configuration 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 SCIEX OS, os arquivos e diretórios devem estar armazenados em uma partição do disco rígido que usa o formato NTFS, que pode controlar e auditar o acesso aos arquivos do SCIEX OS. O sistema de arquivos Tabela de alocação de arquivos (FAT) 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 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.

Para obter mais informações sobre as permissões de arquivos e pastas do 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 SCIEX OS, o licenciamento eletrônico pode ser bloqueado por nó ou baseado em servidor. Para o software Central Administrator Console (CAC), o licenciamento eletrônico só pode ser bloqueado por nó.

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 **Licenses** na janela SCIEX OS.

Nota: Renove a licença antes que ela expire.

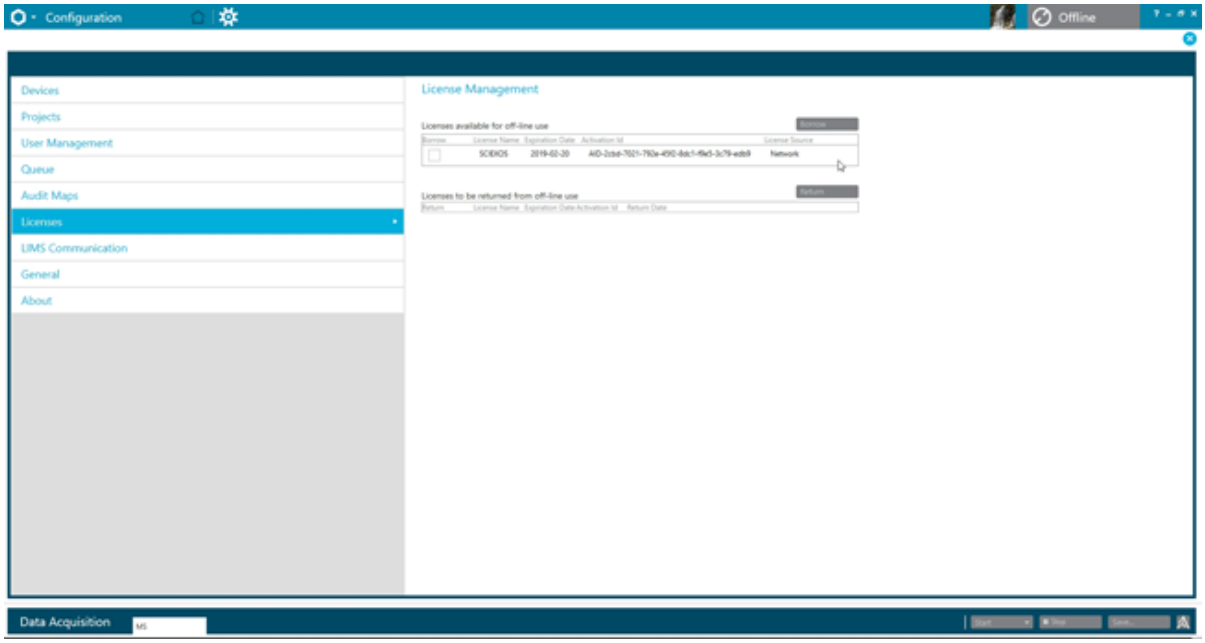
Empréstimo de uma licença eletrônica baseada em servidor

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 Configuration.
2. Clique em **Licenses**.
   A tabela Licenses available for off-line use mostra todas as licenças disponíveis para empréstimo.

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



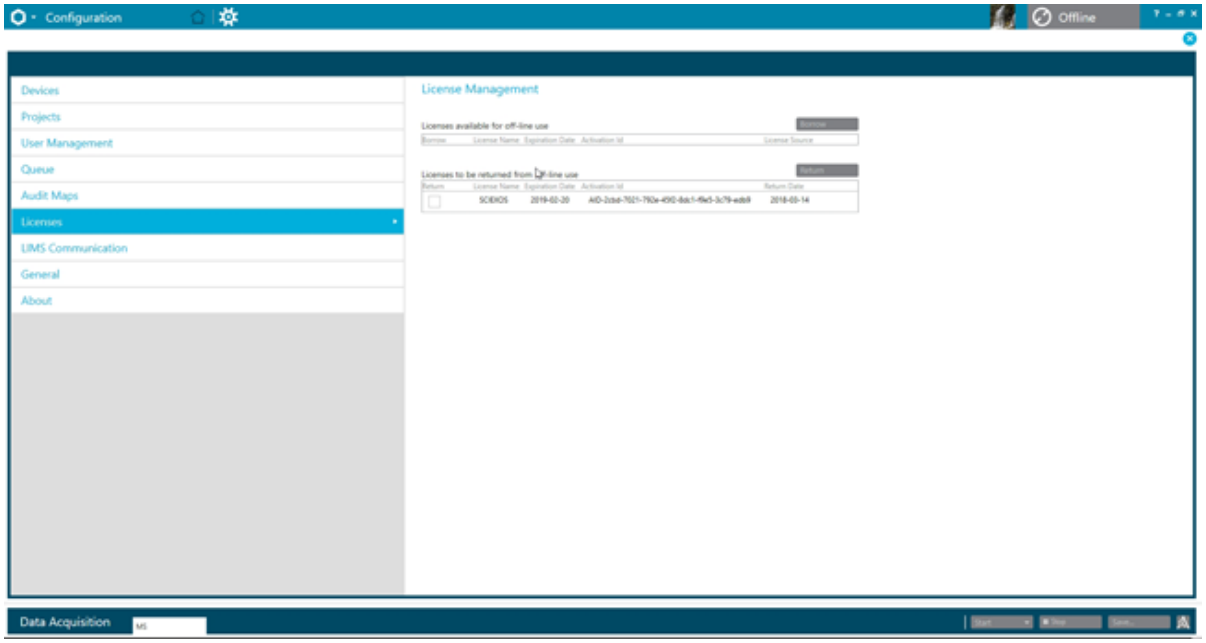
3. Selecione a licença a ser emprestada e, em seguida, clique em **Borrow**.

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 Configuration.
2. Clique em **Licenses**.
   A tabela Licenses to be returned from off-line use 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 **Return**.

Configuração de segurança do software Controle de acesso 4

Esta seção descreve como controlar o acesso ao SCIEX OS. Para controlar o acesso ao SCIEX OS, 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 SCIEX OS.
- Adicione e configure usuários e funções.
- Configure o acesso aos projetos e arquivos de projeto no diretório raiz.

Esse procedimento fornece instruções para a administração local do SCIEX OS. Para uma administração centralizada do 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 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 SCIEX OS: capacidade de abrir o SCIEX OS.
- Autorização do 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 SCIEX OS.	Consulte o documento: *Guia do usuário do software SCIEX OS*.
Configurar o acesso ao SCIEX OS.	Consulte a seção: Configurar acesso ao 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 **SCIEX OS**	
Instale o SCIEX OS.	Sim
Abra o Event Viewer para inspecionar a instalação.	Sim
Segurança do software	
Selecionar o modo de segurança.	Sim
Configurar usuários e funções do 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 SCIEX OS

Antes de instalar o 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 SCIEX OS pode criar mapas de auditoria personalizados e atribuir uma mapa de auditoria diferente no espaço de trabalho Configuration.

Configurar o Security Mode

Esta seção descreve as opções do Security Mode encontradas na página User Management do espaço de trabalho Configuration.

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

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

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 .. 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 SCIEX OS.

Selecionar o Security Mode

1. Abra o espaço de trabalho Configuration.
2. Clique em **User Management**.
3. Clique na guia **Security Mode**.
4. Selecione **Integrated Mode** ou **Mixed Mode**. Consulte a seção: Configurar o Security Mode.
5. Clique em **Save**.
   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 Configuration.
2. Clique em **User Management**.
3. Abra a guia Security Mode.
4. Para configurar o recurso Screen Lock, siga as seguintes etapas:
   a. Selecione **Screen Lock**.
   b. No campo **Wait**, 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 **Auto Logoff**.
   b. No campo **Wait**, 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 **Save**.
   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 Configuration.
2. Clique em **User Management**.
3. Abra a guia Security Mode.
4. Marque a caixa de seleção **Send e-mail messages after** 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 **Send e-mail messages after**.
5. No campo **SMTP Server**, 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 **Port Number**, digite o número da porta aberta.
   Clique em **Apply Default** para inserir o número da porta padrão, 25.
7. No campo **To**, digite o endereço de e-mail para o qual a mensagem deve ser enviada. Por exemplo: nomedeusuário@domínio.com.
8. No campo **From**, digite o endereço de e-mail a ser mostrado no campo **From** da mensagem.
9. No campo **Subject**, digite o assunto da mensagem.
10. No campo **Message**, digite o texto a ser incluído no corpo da mensagem.
11. Clique em **Save**.
    Uma caixa de diálogo de confirmação é aberta.
12. Clique em **OK**.

13. Para verificar a configuração, clique em **Send Test Mail**.

Configurar acesso ao 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 da implementação completa do SCIEX OS.

SCIEX OS Permissões

Figura 4-1: Página User Management

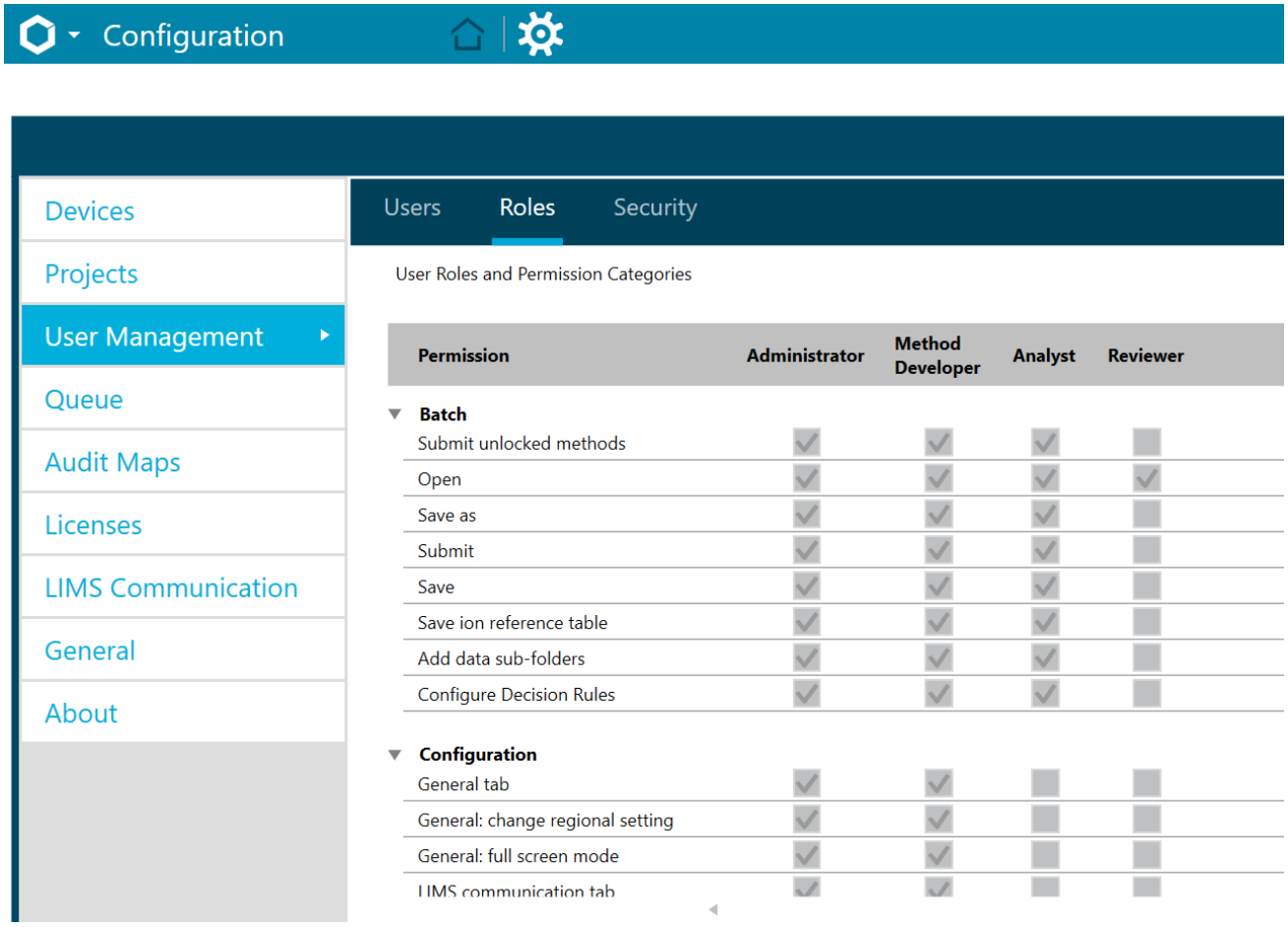


Tabela 4-3: Permissões

Permissão	Descrição
Batch (Lote)	
Submit unlocked methods	(Métodos desbloqueados de envio) Permite que os usuário enviem lotes que contêm métodos desbloqueados.
Open	(Abrir) Permite que os usuários abram lotes existentes.
Save as	(Salvar como) Permite que os usuários salvem lotes com um novo nome.
Submit	(Enviar) Permite que os usuários enviem lotes.
Save	(Salvar) Permite que os usuários salvem um lote, substituindo o conteúdo existente.
Save ion reference table	(Salvar tabela de referência de íons) Permite que os usuários editem a tabela de referência de íons.

Tabela 4-3: Permissões (continuação)

Permissão	Descrição
Add data sub-folders	(Adicionar subpastas de dados) Permite que os usuários criem subpastas para armazenar dados.
Configure Decision Rules	(Configurar regras de decisão) Permite que os usuários adicionem e alterem regras de decisão.
Configuration (Configuração)	
General tab	(Guia Geral) Permite que os usuários abram a página General no espaço de trabalho Configuration.
General: change regional setting	(Geral: alterar configuração regional) Permite que os usuários apliquem configurações regionais do sistema atual ao SCIEX OS.
General: full screen mode	(Geral: modo tela cheia) Permite que os usuários ativem e desativem o modo Full Screen.
General: Stop Windows services	(Geral: Interromper serviços do Windows) Permite que os usuários habilitem ou desabilitem a opção **Windows Settings**.
LIMS communication tab	(Guia Comunicação LIMS) Permite que os usuários abram a página LIMS Communication no espaço de trabalho Configuration.
Audit maps tab	(Guia Mapas de auditoria) Permite que os usuários abram a página Audit Maps no espaço de trabalho Configuration.
Queue tab	(Guia Fila) Permite que os usuários abram a página Queue no espaço de trabalho Configuration.
Queue: instrument idle time	(Fila: tempo de ociosidade do instrumento) Permite que os usuários definam o tempo de ociosidade do instrumento.
Queue: max number of acquired samples	(Fila número máximo de amostras adquiridas) Permite que os usuários definam o número máximo de amostras adquiridas permitidas.
Queue: other queue settings	(Fila: outras configurações de fila) Permite que os usuários configurem outras configurações de fila.
Projects tab	(Guia Projetos) Permite que os usuários abram a página Projects no espaço de trabalho Configuration.
Projects: create project	(Projetos: criar projeto) Permite que os usuários criem projetos.
Projects: apply an audit map template to an existing project	(Projetos: aplicar um modelo de mapa de auditoria a um projeto existente) Permite que os usuários apliquem um mapa de auditoria a um projeto.

Tabela 4-3: Permissões (continuação)

Permissão	Descrição
Projects: create root directory	(Projetos: criar diretório raiz) Permite que os usuários criem um diretório raiz para armazenar projetos.
Projects: set current root directory	(Projetos: definir diretório raiz atual) Permite que os usuários alterem o diretório raiz para um projeto.
Projects: specify network credentials	(Projetos: especificar credenciais de rede) Permite que os usuários especifiquem uma conta de rede segura (SNA) para ser usada durante a aquisição de rede se o usuário com sessão iniciada não tiver acesso ao recurso da rede.
Projects: Enable checksum writing for wiff data creation	(Projetos: habilitar gravação de 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.
Projects: clear root directory	(Projetos: apagar diretório raiz) Permite que os usuários excluam um diretório raiz da lista.
Devices tab	(Guia Dispositivos) Permite que os usuários abram a página Devices no espaço de trabalho Configuration.
User management tab	(Guia Gerenciamento do usuário) Permite que os usuários abram a página User management no espaço de trabalho Configuration.
Force user logoff	(Forçar logoff do usuário) Permite que os usuários forcem o logoff de um usuário que esteja atualmente logado no SCIEX OS. Permite que os usuários forcem o logoff de um usuário que esteja atualmente logado no software SCIEX OS
Event Log (Log de eventos)	
Access event log workspace	(Acessar o espaço de trabalho Event log) Permite que os usuários abram o espaço de trabalho Event Log.
Archive log	(Arquivar registro) Permite que os usuários arquivem o registro de eventos.
Audit Trail (Rastreamento de auditoria)	
Access audit trail workspace	(Acessar espaço de trabalho Audit Trail) Permite que os usuários abram o espaço de trabalho Audit Trail.
View active audit map	(Visualizar mapa de auditoria ativo) Permite que os usuários visualizem os mapas de auditoria ativos de uma estação de trabalho ou projeto no espaço de trabalho Audit Trail.
Print/Export audit trail	(Imprimir/Exportar rastreamento de auditoria) Permite que os usuários imprimam ou exportem o rastreamento de auditoria.

Tabela 4-3: Permissões (continuação)

Permissão	Descrição
CAC Server (Servidor do CAC) (somente CAC)	
Manage Workgroups	(Gerenciar grupos de trabalho) Permite que os usuários criem e gerenciem grupos de trabalho no espaço de trabalho User Management.
Manage Workgroups Projects	(Gerenciar projetos dos grupos de trabalho) Permite que os usuários criem e gerenciem projetos de grupos de trabalho no espaço de trabalho User Management.
Data Acquisition Panel (Painel de aquisição de dados)	
Start	(Iniciar) Permite que os usuários iniciem a aquisição no painel Data Acquisition.
Stop	(Parar) Permite que os usuários interrompam a aquisição no painel Data Acquisition.
Save	(Salvar) Permite que os usuários salvem dados adquiridos com um nome de arquivo diferente no painel Data Acquisition.
MS & LC Method (Método de MS e LC)	
Access method workspace	(Acessar o espaço de trabalho Method) Permite que os usuários abram os espaços de trabalho MS Method e LC Method.
New	(Novo) Permite que os usuários criem métodos MS e LC.
Open	(Abrir) Permite que os usuários abram métodos MS e LC.
Save	(Salvar) Permite que os usuários salvem um método, substituindo o conteúdo existente.
Save as	(Salvar como) Permite que os usuários salvem métodos com um novo nome.
Lock/Unlock method	(Bloquear/Desbloquear método) Permite que os usuários bloqueiem métodos, para evitar edição, e desbloqueiem métodos.
Queue (Fila)	
Manage	(Gerenciar) Permite que os usuários abram o espaço de trabalho Queue.
Start/Stop	(Iniciar/Parar) Permite que os usuários iniciem ou interrompam a fila.
Print	(Imprimir) Permite que os usuários imprimam a fila.
Library (Biblioteca)	

Tabela 4-3: Permissões (continuação)

Permissão	Descrição
Access library workspace	(Acessar espaço de trabalho Library) Permite que os usuários abram o espaço de trabalho Library. Não aplicável ao fluxo de trabalho Quantificação.
CAC settings (Cliente do CAC)	
Enable Central Administration	(Habilitar administração central) Permite que os usuários configurem o SCIEX OS para a administração central com o software Central Administrator Console (CAC).
MS Tune (Ajuste MS)	
Access MS Tune workspace	(Acessar espaço de trabalho MS Tune) Permite que os usuários abram o espaço de trabalho MS Tune.
Advanced MS tuning	(Ajuste MS avançado) (Sistemas X500 QTOF) Permite que os usuários acessem as opções de ajuste avançadas, que incluem otimização do detector, ajuste positivo e negativo da unidade Q1, ajuste positivo e negativo de TOF MS e ajuste alto positivo e negativo de Q1.
Advanced troubleshooting	(Resolução de problemas avançada) Permite que os usuários abram a caixa de diálogo Advanced Troubleshooting.
Quick status check	(Verificação rápida de status) (Sistemas X500 QTOF) Permite que os usuários realizem Verificações rápidas de status positivo e negativo.
Restore instrument data	(Restaurar dados do instrumento) Permite que os usuários restaurem configurações de ajuste salvas anteriormente.
Explorer (Explorador)	
Access Explorer workspace	(Acessar espaço de trabalho Explorer) Permite que os usuários abram o espaço de trabalho Explorer.
Export	(Exportar) Permite que os usuários exportem dados do espaço de trabalho Explorer.
Print	(Imprimir) Permite que os usuários imprimam dados no espaço de trabalho Explorer.
Options	(Opções) Permite que os usuários modifiquem as opções do espaço de trabalho Explorer.
Recalibrate	(Recalibrar) Permite que os usuários recalibrem amostras e espectros no espaço de trabalho Explorer . Não aplicável ao fluxo de trabalho Quantificação.
Analytics (Análise)	

Tabela 4-3: Permissões (continuação)

Permissão	Descrição
New results	(Novos resultados) Permite que os usuários criem Tabelas de resultados.
Create processing method	(Criar método de processamento) Permite que os usuários criem métodos de processamento.
Modify processing method	(Modificar método de processamento) Permite que os usuários modifiquem métodos de processamento.
Allow Export and Create Report of unlocked Results Table	(Permitir exportação e criação de relatório de Results Table desbloqueadas) Permite que os usuários exportem ou gerem um relatório a partir de uma Results Table ou tabela de estatísticas, se a Results Table não estiver bloqueada.
Save results for Automation Batch	(Salvar resultados para lote automático) Permite que a Results Table criada automaticamente no espaço de trabalho Batch seja salva. Essa permissão é necessária para autoprocessamento durante a aquisição.
Change default quantitation method integration algorithm	(Alterar algoritmo de integração do método padrão de quantificação) Permite que os usuários alterem o algoritmo de integração nas configurações padrão do projeto.
Change default quantitation method integration parameters	(Alterar parâmetros de integração do método padrão de quantificação) Permite que os usuários alterem os parâmetros de integração nas configurações padrão do projeto.
Enable project modified peak warning	(Habilitar aviso de pico modificado do projeto) Permite que usuários habilitem a propriedade de aviso de pico modificado para um projeto.
Add samples	(Adicionar amostras) Permite que os usuários adicionem amostras a uma Results Table.
Remove selected samples	(Remover amostras selecionadas) Permite que os usuários removam amostras de uma Results Table.
Export, import, or remove external calibration	(Exportar, importar ou remover a calibração externa) Permite que os usuários exportem ou removam calibrações externas.
Modify sample name	(Modificar nome da amostra) Permite que os usuários modifiquem o nome da amostra na tabela de resultados.
Modify sample type	(Modificar tipo de amostra) Permite que os usuários modifiquem o tipo de amostra, como padrão controle de qualidade (QC) ou desconhecido, na Results Table.
Modify sample ID	(Modificar ID da amostra) Permite que os usuários modifiquem o ID da amostra na Results Table.

Tabela 4-3: Permissões (continuação)

Permissão	Descrição
Modify actual concentration	(Modificar a concentração real) Permite que os usuários modifiquem a concentração real das amostras Standard e QC na Results Table.
Modify dilution factor	(Modificar o fator de diluição) Permite que os usuários modifiquem o fator de diluição na Results Table.
Modify comment fields	(Modificar campos de comentário) Permite que os usuários modifiquem os campos de comentários: • Component Comment • IS Comment • IS Peak Comment • Peak Comment • Sample Comment
Enable manual integration	(Habilitar integração manual) Permite que os usuários realizem a integração manual.
Set peak to Not Found	(Definir pico como Não encontrado) Permite que os usuários configurem um pico para **Not Found**.
Include or exclude a peak from the Results Table	(Incluir ou excluir um pico a partir da Results Table) Permite que os usuários incluam e excluam picos da Results Table.
Regression options	(Opções de regressão) Permite que os usuários alterem as opções de regressão no painel Calibration Curve.
Modify Results Table integration parameters for a single chromatogram	(Modificar os parâmetros de integração da tabela de resultados para um cromatograma único) Permite que os usuários alterem os parâmetros de integração para um cromatograma único no painel Peak Review.
Modify quantitation method for the Results Table component	(Modificar o método de quantificação para o componente Results Table) Permite que os usuários selecionem um método de processamento diferente para um componente no painel Peak Review com a opção **Update Processing Method for Component**.
Create metric plot new settings	(Criar novas configurações de trama métrica) Permite que os usuários criem novas Tramas métricas e alterem as configurações.
Add custom columns	(Adicionar colunas personalizadas) Permite que os usuários adicionem colunas personalizadas a uma tabela de resultados.

Tabela 4-3: Permissões (continuação)

Permissão	Descrição
Set peak review title format	(Definir formado de título de revisão de pico) Permite que os usuários alterem o título da revisão de pico.
Remove custom column	(Remova a coluna personalizada) Permite que os usuários removam colunas personalizadas de uma tabela de resultados.
Results Table display settings	(Configurações de exibição da Results Table) Permite que os usuários personalizem as colunas mostradas na Results Table.
Lock Results Table	(Bloquear Results Table) Permite que os usuários bloqueiem a Results Table para evitar edição.
Unlock Results Table	(Desbloquear Results Table) Permite que os usuários desbloqueiem a Results Table para permitir edição.
Mark Results file as reviewed and save	(Marcar arquivo de resultados como revisado e salvo) Permite os usuários marquem uma Results Table como revisada e salve-a.
Modify report template	(Modificar modelo de relatório) Permite que os usuários alterem os modelos de relatório.
Transfer results to LIMS	(Transferir resultados para o LIMS) Permite que os usuários façam upload dos resultados para um Sistema de gerenciamento de informações laboratoriais (LIMS).
Modify barcode column	(Modificar coluna do código de barras) Permite que os usuários alterem a coluna **Barcode** em uma Results Table.
Change comparison sample assignment	(Alterar atribuição de amostra de comparação) Permite que os usuários alterem a amostra de comparação especificada na coluna **Comparison** da Results Table.
Add the MSMS spectra to library	(Adicionar os espectros MSMS à biblioteca) Permite que os usuários para adicionar os espectros MS/MS selecionados a uma biblioteca. Não aplicável ao fluxo de trabalho Quantificação.
Project default settings	(Configurações padrão do projeto) Permite que os usuários alterem as configurações de processamento quantitativas e qualitativas do projeto padrão.
Create report in all formats	(Criar relatório em todos os formatos) Permite que os usuários gerem relatórios em todos os formatos. Usuários sem essa permissão podem gerar relatórios somente no formato PDF.
Edit flagging criteria parameters	(Editar parâmetros de critérios de alerta) Permite que os usuários alterem os parâmetros de alerta em um método de processamento.

Tabela 4-3: Permissões (continuação)

Permissão	Descrição
Automatic outlier removal parameter change	(Alteração de remoção automática de valor discrepante) Permite que os usuários alterem os parâmetros para remoção automática de valor discrepante.
Enable automatic outlier removal	(Habilitar remoção automática de valor discrepante) Permite que os usuários alterem o método de processamento para ativar o recurso de remoção automática do valor discrepante.
Update processing method via FF/LS	(Atualizar método de processamento via FF/LS) Permite que os usuários atualizem os métodos de processamento usando o Formula Finder e a Library Search. Não aplicável ao fluxo de trabalho Quantificação.
Update results via FF/LS	(Atualizar resultados via FF/LS) Permite que os usuários atualizem os resultados usando o Formula Finder e a Library Search. Não aplicável ao fluxo de trabalho Quantificação.
Enable grouping by adducts functionality	(Habilitar agrupamento através da funcionalidade adutos) Permite que os usuários atualizem o método de processamento para ativar o recurso de agrupamento de adutos.
Browse for files	(Navegar pelos arquivos) Permite que os usuários naveguem fora da pasta local de dados.
Enable standard addition	(Habilitar adição padrão) Permite que os usuários atualizem o método de processamento para ativar o recurso de adição padrão.
Set Manual Integration Percentage Rule	(Configurar regra de porcentagem de integração manual) Permite que os usuários alterem o parâmetro **Manual Integration %**.

Sobre usuários e funções

No SCIEX OS, o administrador pode adicionar os usuários do e os grupos do Windows ao banco de dados User Management para o SCIEX OS. 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.

Os usuários podem ser atribuídos a uma ou mais funções predefinidas, descritas na tabela a seguir, ou a funções personalizadas, se necessário. As funções determinam as funções a que o usuário tem acesso. As funções predefinidas não podem ser excluídas e suas permissões não podem ser alteradas.

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

Tabela 4-4: Funções predefinidas

Função	Tarefas típicas
Administrator (Administrador)	• Gerencia o sistema. • Configura a segurança.
Method Developer (Desenvolvedor de método)	• Cria métodos. • Executa lotes. • Analisa dados para uso do usuário final.
Analyst (Analista)	• Executa lotes. • Analisa dados para uso do usuário final.
Reviewer (Revisor)	• Revisa os dados. • Revisa rastreamentos de auditoria. • Revisa os resultados quantitativos.

Tabela 4-5: Permissões predefinidas

Permissão	Administrador	Desenvolvedor de método	Analyst	Revisor
Batch (Lote)				
Submit unlocked methods (Enviar métodos desbloqueados)	✓	✓	✓	×
Open (Abrir)	✓	✓	✓	✓
Save as (Salvar como)	✓	✓	✓	×
Submit (Enviar)	✓	✓	✓	×
Save (Salvar)	✓	✓	✓	×
Save ion reference table (Saltar tabela de referência de íons)	✓	✓	✓	×
Add data sub-folders (Adicionar subpastas de dados)	✓	✓	✓	×
Configure Decision Rules(Configurar regras de decisão)	✓	✓	✓	×

Tabela 4-5: Permissões predefinidas (continuação)

Permissão	Administrador	Desenvolvedor de método	Analyst	Revisor
Configuration (Configuração)				
General tab (Guia Geral)	✓	✓	×	×
General: change regional setting (Geral: altera a configuração regional)	✓	✓	×	×
General: full screen mode (Geral: modo de tela inteira)	✓	✓	×	×
General: Stop Windows services (Geral: Interromper serviços do Windows)	✓	×	×	×
LIMS communication tab (Guia Comunicação LIMS)	✓	✓	×	×
Audit maps tab (Guia Mapas de auditoria)	✓	×	×	×
Queue tab (Guia Fila)	✓	✓	✓	✓
Queue: instrument idle time (Fila: tempo de ociosidade do instrumento)	✓	✓	×	×
Queue: max number of acquired samples (Fila: número máximo de amostras adquiridas)	✓	✓	×	×
Queue: other queue settings (Fila: outras configurações de fila)	✓	✓	×	×
Projects tab (Guia Projetos)	✓	✓	✓	✓
Projects: create project (Projetos: criar projeto)	✓	✓	✓	×

Tabela 4-5: Permissões predefinidas (continuação)

Permissão	Administrador	Desenvolvedor de método	Analyst	Revisor
Projects: apply an audit map template to an existing project (Projeto: aplicar um modelo de mapa de auditoria a um projeto existente)	✓	×	×	×
Projects: create root directory (Projetos: criar diretório raiz)	✓	×	×	×
Projects: set current root directory (Projetos: definir diretório raiz atual)	✓	×	×	×
Projects: specify network credentials (Projetos: especificar credenciais da rede)	✓	×	×	×
Projects: Enable checksum writing for wiff1 data creation (Projetos: habilite a gravação da soma de verificação para criação de dados wiff1)	✓	×	×	×
Projects: clear root directory (Projetos: apagar diretório raiz	✓	×	×	×
Devices tab (Guia Dispositivos)	✓	✓	✓	×
User management tab (Guia Gerenciamento de usuários)	✓	×	×	×
Force user logoff(Forçar logoff do usuário)	✓	×	×	×
Event Log (Registro de eventos)				

Tabela 4-5: Permissões predefinidas (continuação)

Permissão	Administrador	Desenvolvedor de método	Analyst	Revisor
Access event log workspace (Acessar espaço de trabalho do registro de eventos)	✓	✓	✓	✓
Archive log (Arquivar registro)	✓	✓	✓	✓
Audit Trail (Rastreamento de auditoria)				
Access audit trail workspace (Acessar espaço de trabalho do rastreamento de auditoria)	✓	✓	✓	✓
View active audit map (Visualizar mapa de auditoria ativo)	✓	✓	✓	✓
Print/Export audit trail (Imprimir/Exportar rastreamento de auditoria)	✓	✓	✓	✓
Data Acquisition Panel (Painel de aquisição de dados)				
Start (Iniciar)	✓	✓	✓	×
Stop (Parada)	✓	✓	✓	×
Save (Salvar)	✓	✓	✓	×
MS & LC Method (Método de MS e LC)				
Access method workspace (Acessar espaço de trabalho método)	✓	✓	✓	✓
New (Novo)	✓	✓	×	×
Open (Abrir)	✓	✓	✓	✓
Save (Salvar)	✓	✓	×	×
Save as (Salvar como)	✓	✓	×	×
Lock/Unlock method (Bloquear/Desbloquear método)	✓	✓	×	×

Tabela 4-5: Permissões predefinidas (continuação)

Permissão	Administrador	Desenvolvedor de método	Analyst	Revisor
Queue (Fila)				
Manage (Gerenciar)	✓	✓	✓	×
Start/Stop (Iniciar/Parar)	✓	✓	✓	×
Print (Imprimir)	✓	✓	✓	✓
Library (Biblioteca)				
Access library workspace (Acessar espaço de trabalho biblioteca)	✓	✓	✓	✓
CAC settings (Cliente do CAC)				
Enable Central Administration (Habilitar administração central)	✓	×	×	×
MS Tune (Ajuste MS)				
Access MS Tune workspace (Acessar espaço de trabalho Ajuste MS)	✓	✓	✓	×
Advanced MS Tuning (Ajuste MS avançado)	✓	✓	×	×
Advanced troubleshooting (Resolução de problemas avançada)	✓	✓	×	×
Quick status check (Verificação rápida de status)	✓	✓	✓	×
Restore instrument data (Restaurar dados do instrumento)	✓	✓	×	×
Explorer (Explorador)				

Tabela 4-5: Permissões predefinidas (continuação)

Permissão	Administrador	Desenvolvedor de método	Analyst	Revisor
Access explorer workspace (Acessar espaço de trabalho explorador)	✓	✓	✓	✓
Export (Exportar)	✓	✓	✓	×
Print (Imprimir)	✓	✓	✓	×
Options (Opções)	✓	✓	✓	×
Recalibrate (Recalibrar)	✓	✓	×	×
Analytics (Análise)				
New results (Novos resultados)	✓	✓	✓	×
Create processing method (Criar método de processamento)	✓	✓	✓	×
Modify processing method (Modificar método de processamento)	✓	✓	×	×
Allow Export and Create Report of unlocked Results Table (Permitir exportar e criar relatório da Results Table desbloqueada)	✓	×	×	×
Save results for Automation Batch (Salvar resultados para o lote de automação)	✓	✓	✓	×
Change default quantitation method integration algorithm (Alterar algoritmo de integração de método de quantificação padrão)	✓	✓	×	×

Tabela 4-5: Permissões predefinidas (continuação)

Permissão	Administrador	Desenvolvedor de método	Analyst	Revisor
Change default quantitation method integration parameters (Alterar parâmetros de integração de método de quantificação padrão)	✓	✓	×	×
Enable project modified peak warning (Habilitar aviso de pico modificado do projeto)	✓	×	×	×
Add samples (Adicionar amostras)	✓	✓	✓	×
Remove selected samples (Remover amostras selecionadas)	✓	✓	✓	×
Export, import, or remove external calibration (Exportar, importar ou remover calibração externa)	✓	✓	✓	×
Modify sample name (Modificar nome da amostra)	✓	✓	✓	×
Modify sample type (Modificar tipo da amostra)	✓	✓	✓	×
Modify sample ID (Modificar ID da amostra)	✓	✓	✓	×
Modify actual concentration (Modificar concentração real)	✓	✓	✓	×
Modify dilution factor (Modificar fator de diluição)	✓	✓	✓	×

Tabela 4-5: Permissões predefinidas (continuação)

Permissão	Administrador	Desenvolvedor de método	Analyst	Revisor
Modify comment fields (Modificar campos de comentário)	✓	✓	✓	×
Enable manual integration (Habilitar integração manual)	✓	✓	✓	×
Set peak to not found (Definir pico como não encontrado)	✓	✓	✓	×
Include or exclude a peak from the results table (Incluir ou excluir um pico a partir da tabela de resultados)	✓	✓	✓	×
Regression options (Opções de regressão)	✓	✓	✓	×
Modify results table integration parameters for a single chromatogram (Modificar parâmetros de integração da tabela de resultados para um único cromatograma)	✓	✓	✓	×
Modify quantitation method for the results table component (Modificar o método quantitativo para o componente da tabela de resultados)	✓	✓	✓	×
Create metric plot new settings (Criar novas configurações de trama métrica)	✓	✓	✓	✓
Add custom columns (Adicionar colunas personalizadas)	✓	✓	✓	×

Tabela 4-5: Permissões predefinidas (continuação)

Permissão	Administrador	Desenvolvedor de método	Analyst	Revisor
Set peak review title format (Definir formato de título de análise de pico)	✓	×	×	×
Remove custom column (Remover coluna personalizada)	✓	✓	×	×
Results table display settings (Configurações de exibição da tabela de resultados)	✓	✓	✓	✓
Lock results table (Bloquear tabela de resultados)	✓	✓	✓	✓
Unlock results table (Desbloquear tabela de resultados)	✓	×	×	×
Mark results file as reviewed and save (Marcar arquivo de resultados como revisado e salvo)	✓	×	×	✓
Modify report template (Modificar modelo de relatório)	✓	✓	×	×
Transfer results to LIMS (Transferir resultados para o LIMS)	✓	✓	✓	×
Modify barcode column (Modificar coluna do código de barras)	✓	✓	×	×
Change comparison sample assignment (Alterar atribuição da amostra de comparação)	✓	✓	×	×

Tabela 4-5: Permissões predefinidas (continuação)

Permissão	Administrador	Desenvolvedor de método	Analyst	Revisor
Add the MSMS spectra to library (Adicionar espectros de MSMS à biblioteca)	✓	✓	×	×
Project default settings (Configurações padrão do projeto)	✓	✓	×	×
Create report in all formats (Criar relatórios em todos os formatos)	✓	✓	✓	✓
Edit flagging criteria parameters (Editar parâmetros dos critérios de alerta)	✓	✓	✓	×
Automatic outlier removal parameter change (Alteração do parâmetro de remoção automática do valor discrepante)	✓	✓	×	×
Enable automatic outlier removal (Habilitar remoção automática do valor discrepante)	✓	✓	✓	×
Update processing method via FF/LS (Atualizar método de processamento FF/LS)	✓	✓	×	×
Update results via FF/LS (Atualizar resultados via FF/LS)	✓	✓	×	×
Enable grouping by adducts functionality (Habilitar agrupamento por funcionalidade adutos)	✓	✓	×	×

Tabela 4-5: Permissões predefinidas (continuação)

Permissão	Administrador	Desenvolvedor de método	Analyst	Revisor
Browse for files (Pesquisar arquivos)	✓	✓	✓	✓
Enable standard addition (Habilitar adição padrão)	✓	✓	✓	×
Set Manual Integration Percentage Rule(Definir regra de porcentagem de integração manual)	✓	×	×	×

Gerenciar usuários

Adicionar um usuário ou grupo

1. Abra o espaço de trabalho Configuration.
2. Abra a página User Management.
3. Abra a guia Users.
4. Clique em **Add User** ( ).
   A caixa de diálogo Select User or Group 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 Select User or Group e sobre como usá-la, pressione **F1**.
6. Para tornar o usuário ativo, marque a caixa de seleção **Active user or group**.
7. Na área **Roles**, selecione uma ou mais funções e, em seguida, clique em **Save**.

Desativar usuários ou grupos

1. Abra o espaço de trabalho Configuration.
2. Abra a página User Management.
3. Abra a guia Users.
4. Na lista **User name or group**, selecione o usuário ou grupo a ser desativado.
5. Desmarque a caixa de seleção **Active user or group**.
   O software pede confirmação.
6. Clique em **Yes**.

Remover usuários ou grupos

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

1. Abra o espaço de trabalho Configuration.
2. Abra a página User Management.
3. Abra a guia Users.
4. Na lista **User name or group**, selecione o usuário ou grupo a ser removido.
5. Clique em **Delete**.
   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 Configuration.
2. Abra a página User Management.
3. Abra a guia Users.
4. No campo **User name or group**, 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 **Save**.

Criar uma função personalizada

1. Abra o espaço de trabalho Configuration.
2. Abra a página User Management.
3. Abra a guia Roles.
4. Clique em **Add Role** ().
   A caixa de diálogo Duplicate a User Role é aberta.
5. No campo **Existing user role**, 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 **Save All Roles**.

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 Configuration.
2. Abra a página User Management.
3. Abra a guia Roles.
4. Clique em **Delete a Role**.
   A caixa de diálogo Delete a User Role 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 Gerenciamento do usuário do 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 Configuration.
2. Abra a página User Management.
3. Clique em **Advanced** > **Export User Management settings**.
   A caixa de diálogo Export User Management Settings é aberta.
4. Clique em **Browse**.
5. Busque e selecione a pasta que em que as configurações serão salvas e, em seguida, clique em **Select Folder**.
6. Clique em **Export**.
   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 Configuration.

2. Abra a página User Management.
3. Clique em **Advanced** > **Import User Management settings**.
   A caixa de diálogo Import User Management Settings é aberta.
4. Clique em **Browse**.
5. Busque e selecione o arquivo que contém as configurações a serem importadas; em seguida, clique em **Open**.
   O software verifica que o arquivo é válido.
6. Clique em **Import**.
   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 do usuário, 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 Configuration.
2. Abra a página User Management.
3. Clique em **Advanced** > **Restore previous settings**.
   A caixa de diálogo Restore User Management Settings.
4. Clique em **Yes**.
5. Feche o 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 de 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 tipos de arquivo comuns do 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 SCIEX OS	Várias pastas
lcm	Método de LC	`Acquisition Methods`
msm	MS Method	`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 **Nota:** O 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 software SCIEX OS **Nota:** O SCIEX OS gera tanto arquivos wiff quanto 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 do espectrômetro de massas gerado pelo 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, o software CAC e o SCIEX OS não podem ser instalados na mesma estação de trabalho.

Usuários

Use a página User Management para adicionar os usuários do e os grupos do Windows ao banco de dados User Management para o 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 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 Central Administration.
2. Abra a página User Management.
3. Abra a guia User Pool.
4. Clique em **Add users to the User Pool** ( ).
   A caixa de diálogo Select Users or Groups será 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 Central Administration.
2. Abra a página User Management.
3. Abra a guia User Pool.
4. No painel direito, selecione o usuário ou grupo a ser excluído e, em seguida, clique em **Delete**.
   O software pede confirmação.
5. Clique em **OK**.

Funções e permissões do usuário

Esta seção descreve a página User Roles and Permissions.

Os usuários podem ser atribuídos a uma ou mais funções predefinidas, descritas na tabela a seguir, ou a funções personalizadas, se necessário. As funções determinam as funções a que o usuário tem acesso. As funções predefinidas não podem ser excluídas e suas permissões não podem ser alteradas.

Tabela 5-1: Funções predefinidas

Função	Tarefas típicas
Administrator (Administrador)	• Gerencia o sistema. • Configura a segurança.
Method Developer (Desenvolvedor de método)	• Cria métodos. • Executa lotes. • Analisa dados para uso do usuário final.
Analyst (Analista)	• Executa lotes. • Analisa dados para uso do usuário final.
Reviewer (Revisor)	• Revisa os dados. • Revisa rastreamentos de auditoria. • Revisa os resultados quantitativos.

Tabela 5-2: Permissões predefinidas

Permissão	Administrador	Desenvolve-dor de método	Analyst	Revisor
Batch (Lote)				
Submit unlocked methods (Enviar métodos desbloqueados)	✓	✓	✓	×
Open (Abrir)	✓	✓	✓	✓
Save as (Salvar como)	✓	✓	✓	×
Submit (Enviar)	✓	✓	✓	×
Save (Salvar)	✓	✓	✓	×
Save ion reference table (Saltar tabela de referência de íons)	✓	✓	✓	×
Add data sub-folders (Adicionar subpastas de dados)	✓	✓	✓	×
Configure Decision Rules(Configurar regras de decisão)	✓	✓	✓	×
Configuration (Configuração)				
General tab (Guia Geral)	✓	✓	×	×
General: change regional setting (Geral: altera a configuração regional)	✓	✓	×	×
General: full screen mode (Geral: modo de tela inteira)	✓	✓	×	×
LIMS communication tab (Guia Comunicação LIMS)	✓	✓	×	×
General:Stop Windows services(Geral: Interromper serviços do Windows)	✓	×	×	×

Tabela 5-2: Permissões predefinidas (continuação)

Permissão	Administrador	Desenvolve-dor de método	Analyst	Revisor
Audit maps tab (Guia Mapas de auditoria)	✓	×	×	×
Queue tab (Guia Fila)	✓	✓	✓	✓
Queue: instrument idle time (Fila: tempo de ociosidade do instrumento)	✓	✓	×	×
Queue: max number of acquired samples (Fila: número máximo de amostras adquiridas)	✓	✓	×	×
Queue: other queue settings (Fila: outras configurações de fila)	✓	✓	×	×
Projects tab (Guia Projetos)	✓	✓	✓	✓
Projects: create project (Projetos: criar projeto)	✓	✓	✓	×
Projects: apply an audit map template to an existing project (Projeto: aplicar um modelo de mapa de auditoria a um projeto existente)	✓	×	×	×
Projects: create root directory (Projetos: criar diretório raiz)	✓	×	×	×
Projects: set current root directory (Projetos: definir diretório raiz atual)	✓	×	×	×
Projects: specify network credentials (Projetos: especificar credenciais da rede)	✓	×	×	×

Tabela 5-2: Permissões predefinidas (continuação)

Permissão	Administrador	Desenvolve-dor de método	Analyst	Revisor
Projects: Enable checksum writing for wiff1 data creation (Projetos: habilite a gravação da soma de verificação para criação de dados wiff1)	✓	×	×	×
Projects: clear root directory (Projetos: apagar diretório raiz	✓	×	×	×
Devices tab (Guia Dispositivos)	✓	✓	✓	×
User management tab (Guia Gerenciamento de usuários)	✓	×	×	×
Force user logoff(Forçar logoff do usuário)	✓	×	×	×
Event Log (Registro de eventos)				
Access event log workspace (Acessar espaço de trabalho do registro de eventos)	✓	✓	✓	✓
Archive log (Arquivar registro)	✓	✓	✓	✓
Audit Trail (Rastreamento de auditoria)				
Access audit trail workspace (Acessar espaço de trabalho do rastreamento de auditoria)	✓	✓	✓	✓
View active audit map (Visualizar mapa de auditoria ativo)	✓	✓	✓	✓
Print/Export audit trail (Imprimir/Exportar rastreamento de auditoria)	✓	✓	✓	✓

Tabela 5-2: Permissões predefinidas (continuação)

Permissão	Administrador	Desenvolve-dor de método	Analyst	Revisor
Data Acquisition Panel (Painel de aquisição de dados)				
Start (Iniciar)	✓	✓	✓	×
Stop (Parada)	✓	✓	✓	×
Save (Salvar)	✓	✓	✓	×
MS & LC Method (Método de MS e LC)				
Access method workspace (Acessar espaço de trabalho método)	✓	✓	✓	✓
New (Novo)	✓	✓	×	×
Open (Abrir)	✓	✓	✓	✓
Save (Salvar)	✓	✓	×	×
Save as (Salvar como)	✓	✓	×	×
Lock/Unlock method (Bloquear/Desbloquear método)	✓	✓	×	×
Queue (Fila)				
Manage (Gerenciar)	✓	✓	✓	×
Start/Stop (Iniciar/ Parar)	✓	✓	✓	×
Print (Imprimir)	✓	✓	✓	✓
Library (Biblioteca)				
Access library workspace (Acessar espaço de trabalho biblioteca)	✓	✓	✓	✓
CAC settings (Cliente do CAC)				
Enable Central Administration (Habilitar administração central)	✓	×	×	×
MS Tune (Ajuste MS)				

Tabela 5-2: Permissões predefinidas (continuação)

Permissão	Administrador	Desenvolve-dor de método	Analyst	Revisor
Access MS Tune workspace (Acessar espaço de trabalho Ajuste MS)	✓	✓	✓	×
Advanced MS Tuning (Ajuste MS avançado)	✓	✓	×	×
Advanced troubleshooting (Resolução de problemas avançada)	✓	✓	×	×
Quick status check (Verificação rápida de status)	✓	✓	✓	×
Restore instrument data (Restaurar dados do instrumento)	✓	✓	×	×
Analytics (Análise)				
New results (Novos resultados)	✓	✓	✓	×
Create processing method (Criar método de processamento)	✓	✓	✓	×
Modify processing method (Modificar método de processamento)	✓	✓	×	×
Allow Export and Create Report of unlocked Results Table (Permitir exportar e criar relatório da Results Table desbloqueada)	✓	×	×	×
Save results for Automation Batch (Salvar resultados para o lote de automação)	✓	✓	✓	×

Tabela 5-2: Permissões predefinidas (continuação)

Permissão	Administrador	Desenvolve-dor de método	Analyst	Revisor
Change default quantitation method integration algorithm (Alterar algoritmo de integração de método de quantificação padrão)	✓	✓	×	×
Change default quantitation method integration parameters (Alterar parâmetros de integração de método de quantificação padrão)	✓	✓	×	×
Enable project modified peak warning (Habilitar aviso de pico modificado do projeto)	✓	×	×	×
Add samples (Adicionar amostras)	✓	✓	✓	×
Remove selected samples (Remover amostras selecionadas)	✓	✓	✓	×
Export, import, or remove external calibration (Exportar, importar ou remover calibração externa)	✓	✓	✓	×
Modify sample name (Modificar nome da amostra)	✓	✓	✓	×
Modify sample type (Modificar tipo da amostra)	✓	✓	✓	×
Modify sample ID (Modificar ID da amostra)	✓	✓	✓	×

Tabela 5-2: Permissões predefinidas (continuação)

Permissão	Administrador	Desenvolve-dor de método	Analyst	Revisor
Modify actual concentration (Modificar concentração real)	✓	✓	✓	×
Modify dilution factor (Modificar fator de diluição)	✓	✓	✓	×
Modify comment fields (Modificar campos de comentário)	✓	✓	✓	×
Enable manual integration (Habilitar integração manual)	✓	✓	✓	×
Set peak to not found (Definir pico como não encontrado)	✓	✓	✓	×
Include or exclude a peak from the results table (Incluir ou excluir um pico a partir da tabela de resultados)	✓	✓	✓	×
Regression options (Opções de regressão)	✓	✓	✓	×
Modify results table integration parameters for a single chromatogram (Modificar parâmetros de integração da tabela de resultados para um único cromatograma)	✓	✓	✓	×
Modify quantitation method for the results table component (Modificar o método quantitativo para o componente da tabela de resultados)	✓	✓	✓	×

Tabela 5-2: Permissões predefinidas (continuação)

Permissão	Administrador	Desenvolve-dor de método	Analyst	Revisor
Create metric plot new settings (Criar novas configurações de trama métrica)	✓	✓	✓	✓
Add custom columns (Adicionar colunas personalizadas)	✓	✓	✓	×
Set peak review title format (Definir formato de título de análise de pico)	✓	×	×	×
Remove custom column (Remover coluna personalizada)	✓	✓	×	×
Results table display settings (Configurações de exibição da tabela de resultados)	✓	✓	✓	✓
Lock results table (Bloquear tabela de resultados)	✓	✓	✓	✓
Unlock results table (Desbloquear tabela de resultados)	✓	×	×	×
Mark results file as reviewed and save (Marcar arquivo de resultados como revisado e salvo)	✓	×	×	✓
Modify report template (Modificar modelo de relatório)	✓	✓	×	×
Transfer results to LIMS (Transferir resultados para o LIMS)	✓	✓	✓	×

Tabela 5-2: Permissões predefinidas (continuação)

Permissão	Administrador	Desenvolve-dor de método	Analyst	Revisor
Modify barcode column (Modificar coluna do código de barras)	✓	✓	×	×
Change comparison sample assignment (Alterar atribuição da amostra de comparação)	✓	✓	×	×
Add the MSMS spectra to library (Adicionar espectros de MSMS à biblioteca)	✓	✓	×	×
Project default settings (Configurações padrão do projeto)	✓	✓	×	×
Create report in all formats (Criar relatórios em todos os formatos)	✓	✓	✓	✓
Edit flagging criteria parameters (Editar parâmetros dos critérios de alerta)	✓	✓	✓	×
Automatic outlier removal parameter change (Alteração do parâmetro de remoção automática do valor discrepante)	✓	✓	×	×
Enable automatic outlier removal (Habilitar remoção automática do valor discrepante)	✓	✓	✓	×

Tabela 5-2: Permissões predefinidas (continuação)

Permissão	Administrador	Desenvolve-dor de método	Analyst	Revisor
Update processing method via FF/LS (Atualizar método de processamento FF/LS)	✓	✓	×	×
Update results via FF/LS (Atualizar resultados via FF/LS)	✓	✓	×	×
Enable grouping by adducts functionality (Habilitar agrupamento por funcionalidade adutos)	✓	✓	×	×
Browse for files (Pesquisar arquivos)	✓	✓	✓	✓
Enable standard addition (Habilitar adição padrão)	✓	✓	✓	×
Set Manual Integration Percentage Rule(Definir regra de porcentagem de integração manual)	✓	×	×	×
Explorer (Explorador)				
Access explorer workspace (Acessar espaço de trabalho explorador)	✓	✓	✓	✓
Export (Exportar)	✓	✓	✓	×
Print (Imprimir)	✓	✓	✓	×
Options (Opções)	✓	✓	✓	×
Recalibrate (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 Central Administration.
2. Abra a página User Management.
3. Abra a guia User Roles and Permissions.
4. Clique em **Add Role** ( ).
   A caixa de diálogo Duplicate a User Role é aberta.
5. No campo **Existing user role**, 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 exibida na janela User Roles and Permission Categories.
7. Selecione os privilégios de acesso para a função marcando as caixas de seleção adequadas.
8. Clique em **Save All Roles**.

Excluir uma função personalizada

1. Abra o espaço de trabalho Central Administration.
2. Abra a página User Management.
3. Abra a guia User Roles and Permissions.
4. Clique em **Delete a Role**.
   A caixa de diálogo Delete a User Role é aberta.
5. Selecione a função a ser excluída e, em seguida, clique em **OK**.

Grupos de trabalho

Use a página Workgroup Management 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 não precisar mais de segurança baseada em servidor para 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 Central Administration.
2. Abra a página Workgroup Management.
3. Clique em **Add Workgroup** ().
   A caixa de diálogo Add a Workgroup é aberta.
4. Digite um nome no campo **Workgroup Name**.
5. Digite uma descrição no campo **Description** e clique em **Add**.
   O grupo de trabalho é criado e adicionado ao painel Manage Workgroups and Assignments. 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 Central Administration.
2. Abra a página Workgroup Management.
3. Expanda a lista **Workgroups** e encontre o grupo de trabalho a ser excluído. Clique em **Delete**.
   A caixa de diálogo Delete Workgroup é aberta.
4. Clique em **Yes**.

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 Central Administration.
2. Abra a página Workgroup Management.
3. No painel Manage Workgroups and Assignments, expanda o grupo de trabalho a ser alterado e, em seguida, expanda a lista **Users**.
4. Selecione um usuário ou grupo e, em seguida, clique em **Add** ().

   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 **Save**.

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 Central Administration.
2. Abra a página Workgroup Management.
3. No painel Manage Workgroups and Assignments, expanda o grupo de trabalho a ser alterado e, em seguida, expanda a lista **Users**.
4. Na seção Current Workgroup Membership, atribua ou remova funções na coluna **Assign Roles**.
5. Clique em **Save**.

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 Central Administration.
2. Abra a página Workgroup Management.
3. No painel Manage Workgroups , and Assignments, expanda o grupo de trabalho a ser alterado e, em seguida, expanda a lista **Workstations**.
4. Selecione uma estação de trabalho e, em seguida, clique em **Add** (). A estação de trabalho é adicionada ao grupo de trabalho atual.
5. Clique em **Save**.

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 Central Administration.
2. Abra a página Workgroup Management.
3. No painel Manage Workgroups , and Assignments, expanda o grupo de trabalho a ser alterado e, em seguida, expanda a lista **Workstations**.
4. (Opcional) Para tornar o grupo de trabalho atual o grupo de trabalho padrão para essa estação de trabalho, marque a caixa de seleção **Set Default** na seção Current Workgroup Membership.
5. Na seção Assign Security Settings, selecione o **Security mode** para o grupo de trabalho e, em seguida, digite os tempos de **Screen lock** e **Auto logoff** apropriados.
6. Clique em **Save**.

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 Central Administration.
2. Abra a página Workgroup Management.
3. No painel Manage Workgroups , and Assignments, expanda o grupo de trabalho a ser alterado e, em seguida, expanda a lista **Projects**.
4. Marque a caixa de seleção **Use central settings for projects**.
   A seção de seleção de projetos é exibida.
5. Selecione um **Project root directory** 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 **Add** () para adicionar os projetos ao grupo de trabalho.
   A raiz do projeto é adicionada à tabela Current Workgroup Membership. Expanda a raiz do projeto para exibir os projetos atuais no grupo de trabalho.
7. Clique em **Save**.

Gerenciar projetos

Use a página Project Management 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 de projetos 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 da 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 Central Administration.
2. Abra a página Project Management.
3. Clique em **Add new or existing project root to project pool** ( ).
   A caixa de diálogo Add Root Directory 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 **Browse** 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 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 Central Administration.
2. Abra a página Project Management.
3. Procure o diretório raiz do projeto a ser excluído e, em seguida, clique em **Delete Project Root**, na seção Actions.
   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 Central Administration.
2. Abra a página Project Management.
3. Clique em **Add project**, na seção Actions da pasta raiz.
   A caixa de diálogo New Project 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 Central Administration.
2. Abra a página Project Management.
3. Clique em **Add data sub-folders**, na seção Actions da pasta raiz.
   A caixa de diálogo Add Data Sub-Folders é aberta.
4. Selecione um projeto para ao qual a subpasta pertencerá.
5. Clique em **Add a new data sub-folder** ( ).
   A caixa de diálogo Data Sub-Folder Name se abre.
6. Digite o nome da subpasta.
7. Clique em **Save**.

   Dica! As subpastas podem ser aninhadas em outras subpastas. Para criar uma subpasta aninhada, selecione uma subpasta existente na seção Project Data Sub-Folders e, em seguida, clique em **Add a new data sub-folder** ( ).
8. Feche a caixa de diálogo Add Data Sub-Folders.

Estações de trabalho

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

Adicione uma estação de trabalho

Na página Workstation Management, os administradores podem adicionar ou remover estações de trabalho do controle do software Central Administrator Console (CAC).

1. Abra o espaço de trabalho Central Administration.
2. Abra a página Workstation Management.
3. Clique em **Add Workstation to the Workstations Pool** ().
   A caixa de diálogo Select Computers é aberta.
4. Digite os nomes das estações de trabalho a serem adicionadas e, em seguida, clique em **OK**.

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 estações de trabalho. Excluir uma estação de trabalho a remove dos grupos de trabalho aos quais ela foi atribuída. Nenhum dado é perdido na estação de trabalho quando ela é removida.

1. Abra o espaço de trabalho Central Administration.
2. Abra a página Workstation Management.
3. Clique em **Workstation Management**.
4. No painel Workstation Pool, procure a estação de trabalho a ser excluída e, em seguida, clique em **Delete**.
   A caixa de diálogo Delete Workstation é aberta.
5. Clique em **OK**.

Recursos de relatórios e segurança

Gerar relatórios de dados do grupo de trabalho

Os usuários podem 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 Central Administration.
2. Clique em **Print**.
   A caixa de diálogo Print abrirá.
3. Defina as opções de impressão e, em seguida, clique em **Print**.

4. (Imprimir somente em PDF) Navegue até a localização em que o Relatório será salvo e, em seguida, clique em **Save**.

Exportar configurações do software CAC

O usuário pode exportar as configurações de segurança que podem ser aplicadas a outro servidor Central Administrator Console (CAC). As configurações são exportadas como um arquivo ecac.

1. Abra o espaço de trabalho Central Administration.
2. Clique em **Advanced** > **Export CAC settings**.
   A caixa de diálogo Exportar CAC Settings será aberta.
3. Clique em **Browse**.
4. Busque e selecione a pasta que em que as configurações serão salvas e, em seguida, clique em **Select Folder**.
5. Clique em **Export**.
   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

O usuário pode importar configurações de segurança do SCIEX OS ou outros servidores do Central Administrator Console (CAC). As configurações são importadas como um arquivo ecac.

1. Abra o espaço de trabalho Central Administration.
2. Clique em **Advanced** > **Import CAC settings**.
   A caixa de diálogo Import CAC Settings será aberta.
3. Clique em **Browse**.
4. Busque e selecione o arquivo que contém as configurações a serem importadas; em seguida, clique em **Open**.
   O software verifica que o arquivo é válido.
5. Clique em **Import**.
   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**.

Restaurar configurações do software CAC

O usuário pode importar automaticamente as últimas configurações ecac exportadas.

1. Abra o espaço de trabalho Central Administration.
2. Clique em **Advanced** > **Restore CAC settings**.
   A caixa de diálogo Restore CAC Settings será aberta.

   Nota: As configurações restauradas são aplicadas após o software Central Administrator Console (CAC) ser reiniciado.

3. Clique em **Yes**.

Aquisição de rede 6

Esta seção descreve como a aquisição de rede funciona no SCIEX OS e as vantagens e limitações de projetos baseados em rede. Também contém procedimentos para configuração de aquisição da 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 excluir o acesso a essa pasta, o

SCIEX OS não pode funcionar idealmente. 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 User Management do SCIEX OS.

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

Se uma SNA não for especificada, o SCIEX OS usará as credenciais da conta logada 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 SCIEX OS adquire dados para um local de rede, ele primeiro grava cada amostra em uma pasta na 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 SCIEX OS tenta novamente a cada 15 minutos até que a transferência seja 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 SCIEX OS armazena dados. Para ter certeza de que as informações do projeto estão armazenadas de forma segura, crie o diretório raiz usando o SCIEX OS. Não crie projetos no File Explorer.

Opcionalmente, ao criar os diretórios raízes em um recurso de rede, defina as **Credentials for Secure Network Account**. 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 Configuration.
2. Clique em **Projects**.
3. Na seção **Advanced**, clique em **Credentials for Secure Network Account**.
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

Eventos auditados são armazenados nas trilhas de auditoria. Dois tipos de trilha de auditoria estão disponíveis: estação de trabalho e projeto.

As trilhas de auditoria da estação de trabalho são arquivos que armazenam os eventos auditados para o computador em que o software SCIEX OS ou Central Administrator Console (CAC) está sendo executado. Para obter uma lista completa de eventos auditados, consulte a seção: Rastreamento de auditoria da estação de trabalho.

Uma trilha de auditoria de projeto é o arquivo que armazena os eventos auditados para um projeto. Para obter uma lista completa de eventos auditados, consulte a seção: Rastreamento de auditoria do projeto. No software SCIEX OS e CAC software, o espaço de trabalho Audit Trail mostra as trilhas de auditoria para os projetos no diretório raiz atual. O processamento de eventos de rastreamentos de auditoria está contido no mapa de rastreamento de auditoria e é armazenado com a Results Table.

Rastreamentos de auditoria, combinados com arquivos como os arquivos wiff2 e da Results Table, constituem registros eletrônicos válidos que podem ser usados para propósitos 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

Tabela 7-1: Rastreamentos de auditoria (continuação)

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

Estação de trabalho (CAC)	• Muda para:
	  • Mapa de auditoria
	  • Servidor do 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 Audit Maps do espaço de trabalho Configuration

Depois que a trilha de auditoria da estação de trabalho ou uma trilha de auditoria do projeto contiver 20.000 registros de auditoria, o software SCIEX OS e CAC arquivarão automaticamente os registros e iniciarão uma nova trilha 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. Dois tipos de mapas de auditoria estão disponíveis: estação de trabalho 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 para um projeto pode ser editado no software SCIEX OS ou no Central Administrator Console (CAC).

O usuário pode criar vários mapas de auditoria para estações de trabalho e projetos, mas somente um mapa de auditoria pode ser usado por vez para cada estação de trabalho e

cada projeto. O mapa de auditoria que está sendo usado para uma 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 No Audit Map. 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 são apropriados para os procedimentos operacionais padrão. Vários modelos de mapas de auditoria padrão estão disponíveis quando o software é instalado, mas talvez seja necessário criar um mapa personalizado. Certifique-se de que um mapa de auditoria apropriado está disponível para o rastreamento de auditoria da estação de trabalho e de que um mapa de auditoria apropriado está disponível para cada projeto.

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

Tarefa	Consulte
Criar um mapa de auditoria para o rastreamento de auditoria da estação de trabalho.	• Criação de um mapa de auditoria de estações de trabalho. • Edição de um mapa de auditoria de estações de trabalho.
Aplicar o mapa de auditoria ao rastreamento de auditoria da estação de trabalho.	• Alteração do mapa de auditoria ativo de uma estação de trabalho.
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.
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 **Change Active Audit Map Assignment** 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: 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 Configuration.
2. Clique em **Audit Maps**.
3. Clique na guia Projects Templates.

4. No campo **Edit map template**, selecione um modelo a ser usado como base para o novo mapa.
5. Clique em **Add Template** ( ).
   A caixa de diálogo Add a Project Audit Map Template 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 **Audited** para o evento.
   b. (Opcional) Se um motivo for exigido, selecione **Reason Required**.
   c. (Opcional) Se uma assinatura eletrônica for exigida, selecione **E-Sig Required**.
   d. (Opcional) Se forem exigidos motivos pré-definidos, selecione **Use Predefined Reason Only** e defina os motivos.
8. Certifique-se de que a caixa de seleção **Audited** está desmarcada para qualquer evento que não será auditado.
9. Clique em **Save Template**.
   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 **Yes**, selecione os projetos que usarão o novo mapa e, em seguida, clique em **Apply**.
    - Se o novo mapa não deve ser aplicado aos projetos existentes, clique em **No**.
11. (Opcional) Para utilizar este mapa de auditoria como padrão para todos os novos projetos, clique em **Use as Default for New Projects**.

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 Configuration.
2. Clique em **Audit Maps**.
3. Clique na guia Projects Templates.
4. No campo **Edit map template**, 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 **Audited** para o evento.
   b. (Opcional) Se um motivo for exigido, selecione **Reason Required**.
   c. (Opcional) Se uma assinatura eletrônica for exigida, selecione **E-Sig Required**.
   d. (Opcional) Se forem exigidos motivos pré-definidos, selecione **Use Predefined Reason Only** e defina os motivos.

6. Certifique-se de que a caixa de seleção **Audited** está desmarcada para qualquer evento que não será auditado.
7. Clique em **Save Template**.
   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 **Yes**, selecione os projetos que usarão o novo mapa e, em seguida, clique em **Apply**.
   - Se o novo mapa não deve ser aplicado aos projetos existentes, clique em **No**.

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 Configuration.
2. Clique em **Audit Maps**.
3. Clique na guia Projects Templates.
4. No campo **Edit map template**, selecione o mapa de auditoria a ser atribuído ao projeto.
5. Clique em **Apply to Existing Projects**.
   A caixa de diálogo Apply Project Audit Map Template é aberta.
6. Marque as caixas de seleção dos projetos aos quais será aplicado este mapa de auditoria.
7. Clique em **Apply**.

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 Configuration.
2. Clique em **Audit Maps**.
3. Clique na guia Projects Templates.
4. No campo **Edit map template**, selecione o mapa a ser excluído.
5. Clique em **Delete Template**.
   O sistema pede confirmação.
6. Clique em **Yes**.

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 Configuration.
2. Clique em **Audit Maps**.
3. Clique na guia Workstation Templates.
4. No campo **Edit map template**, selecione um modelo a ser usado como base para o novo mapa.
5. Clique em **Add Template** ().
   A caixa de diálogo Add a Workstation Audit Map Template 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 **Audited** para o evento.
   b. (Opcional) Se um motivo for exigido, selecione **Reason Required**.
   c. (Opcional) Se uma assinatura eletrônica for exigida, selecione **E-Sig Required**.
   d. (Opcional) Se forem exigidos motivos pré-definidos, selecione **Use Predefined Reason Only** e defina os motivos.
8. Certifique-se de que a caixa de seleção **Audited** está desmarcada para qualquer evento que não será auditado.
9. Clique em **Save Template**.
10. (Opcional) Para tornar este mapa de auditoria o mapa de auditoria ativo para a estação de trabalho, clique em **Apply to the Workstation**.

Edição de 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 Configuration.
2. Clique em **Audit Maps**.
3. Clique na guia Workstation Templates.
4. No campo **Edit map template**, 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 **Audited** para o evento.
   b. (Opcional) Se um motivo for exigido, selecione **Reason Required**.
   c. (Opcional) Se uma assinatura eletrônica for exigida, selecione **E-Sig Required**.
   d. (Opcional) Se forem exigidos motivos pré-definidos, selecione **Use Predefined Reason Only** e defina os motivos.

6. Certifique-se de que a caixa de seleção **Audited** está desmarcada para qualquer evento que não será auditado.
7. Clique em **Save Template**.
8. (Opcional) Para tornar este mapa de auditoria o mapa de ativo para a estação de trabalho, clique em **Apply to the Workstation**.

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 Configuration.
2. Clique em **Audit Maps**.
3. Clique na guia Workstation Templates.
4. No campo **Edit map template**, selecione o mapa a ser aplicado à estação de trabalho.
5. Clique em **Apply to the Workstation**.

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 Configuration.
2. Clique em **Audit Maps**.
3. Clique na guia Workstation Templates.
4. No campo **Edit map template**, selecione o mapa a ser excluído.
5. Clique em **Delete Template**.
   O sistema pede confirmação.
6. Clique em **Yes**.

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 um rastreamento de auditoria

1. Abra o espaço de trabalho Audit Trail.
2. Selecione o rastreamento de auditoria a ser visualizado.
   - Para visualizar o rastreamento de auditoria da estação de trabalho, clique em **Workstation**.

- Para visualizar um rastreamento de auditoria de projeto, selecione o projeto.

3. Para exibir detalhes de um registro de auditoria, selecione o registro.

Buscar ou filtrar registros de auditoria

1. Abra o espaço de trabalho Audit Trail.
2. Selecione o rastreamento de auditoria a ser pesquisado.
3. Para pesquisar um registro de auditoria específico, insira o texto no campo **Find in Page**.
   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 Filter Audit Trail 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 mil registros de auditoria, o 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 Audit Trail.
2. Clique em **Browse**.
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 Audit Trail.
2. Selecione o rastreamento de auditoria a ser impresso.
3. Clique em **Print**.
   A caixa de diálogo Print 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 Audit Trail.
2. Selecione o rastreamento de auditoria a ser exportado.
3. Clique em **Export**.
4. Navegue até o local em que o arquivo exportado será armazenado, insira um **File name** e, em seguida, clique em **Save**.
   O rastreamento de auditoria é salvo como um arquivo csv (valores separados por vírgulas).

Registros de rastreamento de auditoria

Esta seção descreve os campos nos registros de trilha 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 7-4: Campos para registro de eventos

Campo	Descrição
Timestamp	Data e hora do registro.
Event Name	Módulo que gerou o evento.
Descrição	Descrição do evento.
Reason	Razão da alteração, especificada pelo usuário, se necessário.
E-signature	Se uma assinatura eletrônica foi fornecida.
Full User Name	Nome completo do usuário.
Usuário	UPN (user principal name) do usuário.
Category	Tipo de evento.

Para listas de todos os eventos que são gravados na estação de trabalho e nas trilhas de auditoria de projetos, consulte as seções: Rastreamento de auditoria da estação de trabalho 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-<*workstation name*>-<*YYYY*><*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 interrupções 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 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 Queue.
2. Parar a fila.
3. Cancele todas as amostras restantes no lote que contém as amostras a serem removidas.
4. Feche o 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. Inicie o SCIEX OS.
   Em 15 minutos, o 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.

Eventos de auditoria B

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. O Rastreamento de auditoria do projeto é armazenado 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 **Silent Audit Map**.

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

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

SCIEX OS ou CAC	Software Analyst
Espaço de trabalho Analytics	
Actual Concentration changed	Eventos de quantificação: "Concentration" foi alterado
Auto-Processing File saved	—
Barcode ID changed	—
Comparison sample changed in non-targeted workflow	—
Custom columns modified	Eventos de quantificação: "Custom Title" foi alterado
Data exploration opened	Eventos do projeto: o arquivo de dados foi aberto
Data exported	—
Data transferred to LIMS	—
Dilution Factor changed	Eventos de quantificação: "Dilution Factor" foi alterado
External calibration changed	—
External calibration exported	—

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

SCIEX OS ou CAC	Software Analyst
File saved	Eventos do projeto: A Results Table de quantificação foi criada, a Results Table de quantificação foi modificada, Eventos de quantificação: a Results Table foi salva
Formula column changed	Eventos de quantificação: o nome da fórmula foi alterado, o nome da fórmula foi adicionado, a cadeia da fórmula foi alterada, a coluna da fórmula foi removida
Integration cleared	—
Integration parameters changed	Eventos de quantificação: o pico de quantificação foi integrado
Library search result changed	—
Manual Integration	Eventos de quantificação: o pico de quantificação foi integrado
Manual Integration reverted	Eventos de quantificação: o pico de quantificação foi revertido para o original
MS/MS selection changed	—
Processing method changed and applied	Eventos de quantificação: o método de quantificação foi alterado
Report created	Eventos de projeto: imprimindo documento na impressora, impressão de documento na impressora finalizada
Results Table approved	Eventos de quantificação: o revisor de QA acessou uma tabela de resultados
Results Table created	Eventos de quantificação: a Results Table foi criada
Results Table locked	—
Results Table unlocked	—
Sample ID changed	Eventos de quantificação: "Sample ID" foi alterado
Sample Name changed	Eventos de quantificação: "Sample Name" foi alterado
Samples added or removed	Eventos de quantificação: os arquivos foram adicionados à Results Table, os arquivos foram removidos da Results Table, as amostras foram adicionadas/removidas

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

SCIEX OS ou CAC	Software Analyst
Sample Type changed	Eventos de quantificação: "Sample Type" foi alterado
Std. Addition Actual concentration changed	—
Used column selection changed	Eventos de quantificação: "Use It" foi alterado
Window/pane printed	Eventos de projeto: imprimindo documento na impressora, impressão de documento na impressora finalizada
Página Audit Map	
Project Audit Map changed	Eventos de projeto: as configurações do projeto foram alteradas
Project Audit Trail Printed	—
Project Audit Trail Exported	—
Espaço de trabalho Batch	
Batch information imported from LIMS/ text	—
Print	Eventos de projeto: imprimindo documento na impressora, impressão de documento na impressora finalizada
Espaço de trabalho Explorer	
Open Sample(s)	Eventos do projeto: o arquivo de dados foi aberto
Recalibrate sample(s)	—
Recalibrate sample(s) started	—
Espaço de trabalho LC Method	
Print	Eventos de projeto: imprimindo documento na impressora, impressão de documento na impressora finalizada
Espaço de trabalho MS Method	
Print	Eventos de projeto: imprimindo documento na impressora, impressão de documento na impressora finalizada
Espaço de trabalho Queue	

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

SCIEX OS ou CAC	Software Analyst
Sample Transferred	—

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 **Silent Audit Map**.

Os eventos da trilha de auditoria da estação de trabalho são exibidos no software CAC e no SCIEX OS.

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

SCIEX OS ou CAC	Software Analyst
Instrument Tune (SCIEX OS)	
Firmware changed	—
Manual Tuning	Eventos de instrumento: as configurações do parâmetro de ajuste foram alteradas
Automatic Tuning	Eventos de instrumento: as configurações do parâmetro de ajuste foram alteradas
Print Procedure Result in MS Tune	Eventos de projeto: imprimindo documento na impressora, impressão de documento na impressora finalizada
Hardware Configuration (SCIEX OS)	
Devices Activated	Eventos de instrumento: o perfil de hardware foi ativado
Devices Deactivated	Eventos de instrumento: o perfil de hardware foi desativado
Data File Checksum (SCIEX OS)	
Wiff data file checksum has been changed	—
Espaço de trabalho Explorer (SCIEX OS)	
Open Sample(s)	Eventos do projeto: o arquivo de dados foi aberto

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

SCIEX OS ou CAC	Software Analyst
Recalibrate samples(s)	—
Recalibrate samples(s) started	—
Página Audit Map[1]	
Workstation Audit Map changed	Eventos de instrumento: As configurações do instrumento foram alteradas
Workstation Audit Trail printed	—
Workstation Audit Trail exported	—
CAC Server (CAC)	
Project settings enabled/disabled in a workgroup	—
Project assigned/unassigned to a workgroup	—
User Role(s) assigned/unassigned to user(s) in workgroup	—
User(s)/UserGroup(s) assigned/ unassigned to a workgroup	—
Workgroup added/deleted	—
Workgroup renamed	—
Workstation(s) assigned/unassigned to a workgroup	—
Espaço de trabalho Queue (SCIEX OS)	
Sample moved in Queue	Eventos de instrumento: Amostra movida da posição x para a posição y do Arquivo em lote
Batch moved in Queue	Eventos de instrumento: Mover lote
Reaquiring sample	Eventos de instrumento: Reaquisição de amostra(s)
Sample starts to acquire	—
Print Queue	Eventos de projeto: imprimindo documento na impressora, impressão de documento na impressora finalizada

[1] Esses eventos são gravados no SCIEX OS e no CAC.

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

SCIEX OS ou CAC	Software Analyst
Sample acquistion has completed	Eventos de projeto: A amostra foi adicionada ao arquivo de dados
Automatic reinjections Occurred	—
Automatic injection Occurred	—
Segurança[1]	
Auto logoff by system	Eventos de instrumento: Usuário com sessão encerrada
Forced logoff by another user	Eventos de instrumento: Usuário com sessão encerrada
Forced Logoff failed	—
Screen unlock failed	—
Secure Network Account credentials have been changed	Eventos de instrumento: Conta de aquisição alterada
Secure Network Account credentials have been removed	Eventos de instrumento: Conta de aquisição alterada
Secure Network Account credentials have been specified	Eventos de instrumento: Conta de aquisição alterada
Security configuration changed	Eventos de instrumento: A configuração de segurança foi modificada, Tela de bloqueio alterada, Encerramento de sessão automático alterado
User added/deleted	Eventos de instrumento: Usuário adicionado, Usuário excluído
User has logged in	Eventos de instrumento: Usuário com sessão iniciada
User has logged out	Eventos de instrumento: Usuário com sessão encerrada
User has turned off exclusive mode	—
User Login Failed	Eventos de instrumento: Início de sessão malsucedido
User management settings have been exported	—
User management settings have been imported	—

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

SCIEX OS ou CAC	Software Analyst
User management settings have been restored	—
User role assigned to user/user group	Eventos de instrumento: Usuário alterado, Tipo de usuário
User role deleted	Eventos de instrumento: Tipo de usuário excluído
User role modified	Eventos de instrumento: Tipo de usuário alterado
UserLog[1]	
Print Event Log	—

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

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. Ela mostra as permissões de software Analyst que correspondem às permissões do SCIEX OS.

Tabela C-1: Mapeamento de permissões

SCIEX OS	Software Analyst
Espaço de trabalho Batch	
Submit unlocked methods	—
Open	Lote: Abrir lotes existentes
Save as	Lote: Criar novos lotes, Importar, Editar lotes, Salvar lotes, Substituir lotes
Submit	Lote: Enviar lotes
Save	Lote: Salvar lotes, Substituir lotes
Save ion reference table	—
Add data sub-folders	—
Configure Decision Rules	—
Espaço de trabalho Configuration	
General tab	—
General: change regional setting	—
General: full screen mode	—
General: Stop Windows services	—
LIMS Communication tab	—
Audit maps tab	Gestor da trilha de auditoria: Alterar configurações da trilha de auditoria, Criar ou modificar mapas de auditoria
Queue tab	—
Queue: instrument idle time	—
Queue: max. number of acquired samples	—
Queue: other queue settings	—
Projects tab	—

Tabela C-1: Mapeamento de permissões (continuação)

SCIEX OS	Software Analyst
Projects: create project	Aplicação do Analyst: Criar projeto
Projects: apply an audit map template to an existing project	Gestor da trilha de auditoria: Alterar configurações da trilha de auditoria
Projects: create root directory	Aplicação do Analyst: Criar diretório raiz
Project: set current root directory	Aplicação do Analyst: Configurar diretório raiz
Projects: specify network credentials	—
Projects: Enable checksum writing for wiff data creation	—
Projects: clear root directory	—
Devices tab	Configuração de hardware: Criar, Excluir, Editar, Ativar/Desativar
User management tab	Security Config
Force user logoff	Unlock/Logout Application
Espaço de trabalho Event Log	
Access event log workspace	—
Archive log	—
Espaço de trabalho Audit Trail	
Access audit trail workspace	Gestor da trilha de auditoria: Visualizar dados da trilha de auditoria
View active audit map	Gestor da trilha de auditoria: Visualizar dados da trilha de auditoria
Print/Export audit trail	Gestor da trilha de auditoria: Visualizar dados da trilha de auditoria
Painel Data Acquisition	
Start	—
Stop	—
Save	—
Espaços de trabalho MS Method e LC Method	
Access method workspace	—
New	Método de aquisição: Criar/Salvar método de aquisição

Tabela C-1: Mapeamento de permissões (continuação)

SCIEX OS	Software Analyst
Open	Método de aquisição: Abrir métodos de aquisição como somente leitura (modo de aquisição)
Save	Método de aquisição: Substituir métodos de aquisição, Criar/Salvar método de aquisição
Save as	Método de aquisição: Substituir métodos de aquisição, Criar/Salvar método de aquisição
Lock/Unlock method	—
Espaço de trabalho Queue	
Manage	Fila de amostras: Readquirir, Excluir amostra ou lote, Mover lote
Start/Stop	Fila de amostras: Iniciar amostra, Parar amostra, Abortar amostra, Parar fila
Print	Editor de modelo de relatório: Imprimir
Espaço de trabalho Library	
Access library workspace	Explorar: Configuração da localização da biblioteca, Configuração das opções do usuário, Adicionar registro da biblioteca, Adicionar espectro à biblioteca, Modificar registro da biblioteca (substitui adicionar/excluir se estiver desabilitado), Excluir espectro de MS, Excluir espectro de UV, Excluir estrutura, Visualizar biblioteca, Pesquisa na biblioteca
Configurações do CAC	
Enable Central Administration	—
Espaço de trabalho MS Tune	
Access MS Tune workspace	—
Advanced MS tuning	Ajuste: Otimização do instrumento, Ajuste manual, Editar opções de ajuste
Advanced troubleshooting	—
Quick status check	Ajuste: Opç do instrumento
Restore instrument data	Ajuste: Editar opções de ajuste, Editar dados do instrumento
Espaço de trabalho Explorer	

Tabela C-1: Mapeamento de permissões (continuação)

SCIEX OS	Software Analyst
Access explorer workspace	—
Export	Explorar: Salvar dados para o arquivo de texto
Print	Editor de modelo de relatório: Imprimir
Options	—
Recalibrate	Ajuste: Calibrar a partir do espectro atual
Espaço de trabalho Analytics	
New results	Quantificação: Criar novas tabelas de resultados
Create processing method	Quantificação: Criar métodos de quantificação
Modify processing method	Quantificação: Modificar métodos existentes
Allow Export and Create Report of unlocked Results Table	—
Save results for Automation Batch	—
Change default quantitation method integration algorithm	Quantificação: Alterar opções do método padrão
Change default quantitation method integration parameters	Quantificação: Alterar opções do método padrão
Enable project modified peak warning	—
Add samples	Quantificação: Adicionar ou remover amostras da tabela de resultados
Remove selected samples	Quantificação: Adicionar ou remover amostras da tabela de resultados
Export, import or remove external calibration	—
Modify sample name	Quantificação: Modificar nome da amostra
Modify sample type	Quantificação: Modificar tipo da amostra
Modify sample ID	Quantificação: Modificar ID da amostra
Modify actual concentration	Quantificação: Modificar concentração do analito
Modify dilution factor	Quantificação: Modificar fator de diluição
Modify comments fields	Quantificação: Modificar comentário da amostra

Tabela C-1: Mapeamento de permissões (continuação)

SCIEX OS	Software Analyst
Enable manual integration	Quantificação: Integrar manualmente
Set peak to not found	—
Include or exclude a peak from the results table	Quantificação: Excluir padrões da calibração
Regression options	Quantificação: Alterar parâmetros de regressão
Modify the results table integration parameters for a single chromatogram	Quantificação: Alterar parâmetros "simples" na revisão de pico, Alterar parâmetros "avançados" na revisão de pico
Modify quantitation method for results table component	Quantificação: Editar método das tabelas de resultados
Create metric plot new settings	Quantificação: Modificar ou criar configurações de gráfico de métricas
Add custom columns	Quantificação: Criar ou modificar colunas de fórmula
Set peak review title format	—
Remove custom column	Quantificação: Criar ou modificar colunas de fórmula
Results table display settings	Quantificação: Alterar precisão da coluna da tabela de resultados, Alterar visibilidade da coluna da tabela de resultados, Modificar configurações da tabela de resultados
Lock results table	—
Unlock results table	—
Mark results file as reviewed and save	—
Modify report template	Editor de modelo de relatório: Criar/Modificar modelos de relatório
Transfer results to LIMS	—
Modify barcode column	—
Change comparison sample assignment	—
Add the MSMS spectra to library	Explorar: Adicionar espectro ao registro da biblioteca
Project default settings	Quantificação: Modificar configurações globais (padrão)
Create report in all formats	—

Tabela C-1: Mapeamento de permissões (continuação)

SCIEX OS	Software Analyst
Edit flagging criteria parameters	—
Automatic outlier removal parameter change	—
Enable automatic outlier removal	—
Update processing method via FF/LS	—
Update results via FF/LS	—
Enable grouping by adducts functionality	Quantificação: Criar grupos de analitos, Modificar grupos de analitos
Browse for files	—
Enable standard addition	—
Set Manual Integration Percentage Rule	Quantificação: Habilitar ou desabilitar regra percentual na Integração manual

Soma de verificação de arquivo de dados D

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 Configuration.
2. Clique em **Projects**.
3. Se necessário, expanda **Data File Security**.
4. Para habilitar o recursos de soma de verificação do arquivo de dados, marque a caixa de seleção **Enable checksum writing for wiff data creation**. 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

SCIEX Support

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 visualizar este documento eletronicamente é necessário 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 o produto de hardware, consulte o DVD de documentação para o sistema ou 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.