SCIEX
The Power of Precision

Logiciel SCIEX OS

Guide du directeur de laboratoire

RUO-IDV-05-7370-FR-L

Août 2023

Ce document est fourni aux clients qui ont acheté un équipement SCIEX afin de les informer sur le fonctionnement de leur équipement SCIEX. Ce document est protégé par les droits d'auteur et toute reproduction de tout ou partie de son contenu est strictement interdite, sauf autorisation écrite de SCIEX.

Le logiciel éventuellement décrit dans le présent document est fourni en vertu d'un accord de licence. Il est interdit de copier, modifier ou distribuer un logiciel sur tout support, sauf dans les cas expressément autorisés dans le contrat de licence. En outre, l'accord de licence peut interdire de décomposer un logiciel intégré, d'inverser sa conception ou de le décompiler à quelque fin que ce soit. Les garanties sont celles indiquées dans le présent document.

Certaines parties de ce document peuvent faire référence à d'autres fabricants ou à leurs produits, qui peuvent comprendre des pièces dont les noms sont des marques déposées ou fonctionnent comme des marques de commerce appartenant à leurs propriétaires respectifs. Cet usage est destiné uniquement à désigner les produits des fabricants tels que fournis par SCIEX intégrés dans ses équipements et n'induit pas implicitement le droit et/ou l'autorisation de tiers d'utiliser ces noms de produits comme des marques commerciales.

Les garanties fournies par SCIEX se limitent aux garanties expressément offertes au moment de la vente ou de la cession de la licence de ses produits. Elles sont les uniques représentations, garanties et obligations exclusives de SCIEX. SCIEX ne fournit aucune autre garantie, quelle qu'elle soit, expresse ou implicite, notamment quant à leur qualité marchande ou à leur adéquation à un usage particulier, en vertu d'un texte législatif ou de la loi, ou découlant d'une conduite habituelle ou de l'usage du commerce, toutes étant expressément exclues, et ne prend en charge aucune responsabilité ou passif éventuel, y compris des dommages directs ou indirects, concernant une quelconque utilisation effectuée par l'acheteur ou toute conséquence néfaste en découlant.

Réservé exclusivement à des fins de recherche. Ne pas utiliser dans le cadre de procédures de diagnostic.

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

Table des matières

Introduction 1

Les informations contenues dans le présent manuel visent principalement deux types de public :

- L'administrateur du laboratoire, en charge du fonctionnement et de l'utilisation au quotidien du logiciel SCIEX OS et des instruments associés dans une perspective fonctionnelle.
- L'administrateur du système, chargé de la sécurité du système, de l'intégrité du système et des données.

Présentation de la configuration de sécurité 2

Cette section décrit de quelle manière les composants d'audit et de contrôle d'accès du logiciel SCIEX OS fonctionnent avec les composants d'audit et de contrôle d'accès de Windows. En outre, elle décrit comment configurer la sécurité Windows avant l'installation du logiciel SCIEX OS.

Sécurité et conformité réglementaire

Le logiciel SCIEX OS intègre :

- Une gestion personnalisable pour répondre aux exigences relatives à la recherche et aux exigences réglementaires.
- Des outils de sécurité et d'audit pour prendre en charge la conformité à la norme 21 CFR Part 11 pour l'utilisation des enregistrements électroniques.
- Une gestion flexible et efficace de l'accès à des fonctions critiques du spectromètre de masse.
- Un accès contrôlé et audité à des données et des rapports vitaux.
- Une gestion facile de la sécurité en lien avec la sécurité Windows.

Exigences en matière de sécurité

Les exigences en matière de sécurité englobent des environnements relativement ouverts tels que des laboratoires de recherche ou universitaires, ainsi que des laboratoires aux réglementations plus strictes tels que des laboratoires médico-légaux.

Windows et logiciel SCIEX OS : des sécurités complémentaires

Le logiciel SCIEX OS et le Windows New Technology File System (NTFS) sont dotés de fonctions de sécurité conçues pour contrôler le système et l'accès aux données.

La sécurité Windows fournit le premier niveau de protection en exigeant que les utilisateurs se connectent au réseau à l'aide d'un identifiant et d'un mot de passe uniques. Ainsi, seuls les utilisateurs reconnus par les paramètres de sécurité du réseau ou locaux de Windows ont accès au système. Pour plus d'informations, consultez la section Configuration de la sécurité Windows.

Le logiciel SCIEX OS propose les modes d'accès sécurisés suivants au système :

- mode Mixed
- mode Integrated (paramètre par défaut)

Pour plus d'informations sur les modes et les paramètres de sécurité, consultez la section Configurer le mode de sécurité.

SCIEX OS fournit également des rôles totalement configurables, distincts des groupes d'utilisateurs associés à Windows. L'utilisation des rôles permet au directeur du laboratoire de contrôler l'accès au logiciel et au spectromètre de masse fonction par fonction. Pour plus d'informations, consultez la section Configurer l'accès au logiciel SCIEX OS.

Registres d'audit dans le logiciel SCIEX OS et Windows

Les fonctions d'audit dans le logiciel SCIEX OS, ainsi que les composants d'audit intégrés dans Windows, sont essentiels pour créer et gérer les enregistrements électroniques.

SCIEX OS offre un système de registres d'audit pour répondre aux exigences en matière d'enregistrements électroniques. Les différents registres d'audit enregistrent les éléments suivants :

- Les modifications apportées au tableau d'étalonnage de la masse ou au tableau de résolution, les modifications de configuration du système et les événements de sécurité.
- Les événements de création et de modification de projet, d'ajustement, de lots, de données, de méthodes de traitement et de fichiers de modèle de rapport, ainsi que les événements d'ouverture et de fermeture de module et les événements d'impression. Les événements de suppression enregistrés dans le registre d'audit comprennent la suppression de rôles et la suppression d'utilisateurs dans SCIEX OS.
- Création et modification des informations sur les échantillons, des paramètres d'intégration des pics et de la méthode de traitement intégrée dans un tableau de résultats.

Pour obtenir une liste complète des événements d'audit, consultez la section Événements d'audit.

Le logiciel SCIEX OS utilise le journal d'événements de l'application pour obtenir des informations sur le fonctionnement du logiciel. Utilisez ce journal comme aide au dépannage. Il contient des informations détaillées sur le spectromètre de masse, l'appareil et les interactions avec le logiciel.

Windows conserve des journaux d'événements qui recueillent divers événements liés à la sécurité, au système et aux applications. Dans la plupart des cas, l'audit de Windows sert à recueillir des événements exceptionnels tels qu'un échec de connexion. L'administrateur peut configurer le système pour recueillir un grand nombre d'événements tels que l'accès à des fichiers donnés ou les activités d'administration de Windows. Pour plus d'informations, consultez la section Audits du système.

Conseils de sécurité aux clients : sauvegardes

La sauvegarde des données client relève de la responsabilité du client. Bien que le personnel d'intervention et d'assistance SCIEX puisse proposer des conseils et des recommandations concernant la sauvegarde des données utilisateur, il incombe au client de s'assurer que les données soient sauvegardées conformément aux politiques, besoins et exigences réglementaires du client. La fréquence et la couverture de la sauvegarde

des données client devraient être proportionnées aux exigences organisationnelles et à l'importance des données générées.

Les clients doivent s'assurer que les sauvegardes soient fonctionnelles car les sauvegardes sont un élément important de la gestion globale des données et essentielles à la restauration en cas d'attaque malveillante ou de panne de matériel ou de logiciels. Ne sauvegardez pas l'ordinateur pendant l'acquisition des données, ou veillez à ce que les fichiers acquis soient ignorés dans le logiciel de sauvegarde. Nous recommandons vivement de réaliser une sauvegarde complète de l'ordinateur avant toute mise à jour de sécurité ou toute réparation sur l'ordinateur. Cela facilitera une restauration dans l'éventualité peu probable où un correctif de sécurité affecterait le fonctionnement d'une application.

Norme 21 CFR Part 11

Le logiciel SCIEX OS possède des commandes techniques pour être conforme à la norme 21 CFR Part 11 avec la mise en place de :

- la sécurité en mode Mixed et Integrated liée à la sécurité de Windows,
- l'accès contrôlé aux fonctionnalités par le biais de rôles personnalisables,
- des registres d'audit pour le fonctionnement de l'instrument, l'acquisition des données, l'examen des données et la génération de rapports,
- les signatures électroniques qui utilisent à la fois un ID utilisateur et un mot de passe,
- une configuration adéquate du système d'exploitation Windows,
- des procédures et une formation adéquates au sein de l'entreprise.

Le logiciel SCIEX OS est conçu pour être utilisé avec un système conforme à la norme 21 CFR Part 11. Il peut être configuré de manière à être conforme à cette dernière. La conformité de l'utilisation du logiciel SCIEX OS à la norme 21 CFR Part 11 dépend de l'utilisation de la licence CFR SCIEX OS facultative et de la configuration du logiciel SCIEX OS. Les politiques et procédures nécessaires, ainsi que les formations requises, doivent également être en place dans le laboratoire.

Des services de validation sont disponibles auprès de l'équipe des services professionnels de SCIEX. Pour plus d'informations, contactez complianceservices@sciex.com.

Remarque : Ne laissez pas le logiciel Instrument Settings Converter sur un système validé. Il doit servir au transfert initial des paramètres de l'instrument du logiciel Analyst au logiciel SCIEX OS. Veillez à retirer le logiciel Instrument Settings Converter de l'ordinateur après l'avoir utilisé.

Configuration du système

Le système est en général configuré par des administrateurs réseau ou des personnes disposant de droits d'administration réseau ou locaux.

Configuration de la sécurité Windows

Cette section fournit des consignes pour configurer Windows :

- Respectez ces consignes pour les comptes et le mot de passe Windows :
  - Le mot de passe Windows doit être modifié tous les 90 jours.
  - Le mot de passe Windows ne peut pas être réutilisé au moins lors de l'itération suivante. Le nouveau mot de passe ne peut pas être identique à l'ancien.
  - Le mot de passe Windows doit comporter au minimum huit caractères.
  - Le mot de passe Windows doit respecter au minimum deux des quatre conditions de complexité suivantes :
    - Un caractère alphanumérique en majuscule
    - Un caractère alphanumérique en minuscule
    - Une valeur numérique
    - Un caractère spécial (ex : ! @ # $ % ^ &)
  - Le nom d'utilisateur Windows ne doit pas être **admin**, **Administrateur** ni **démo**.
- Vérifiez que l'administrateur du logiciel SCIEX OS a le droit de modifier les autorisations des fichiers dans le dossier `SCIEX OS Data`. Si ce dossier se trouve sur un ordinateur local, nous suggérons que l'administrateur du logiciel fasse partie du groupe des administrateurs locaux.
- Pour que tous les utilisateurs aient l'accès requis aux ressources en vue de l'acquisition réseau, demandez à l'administrateur réseau d'ajouter un compte réseau sécurisé (SNA) sur la ressource réseau. Ce compte doit avoir des autorisations d'écriture pour le dossier réseau contenant le répertoire racine. Il est défini comme compte réseau sécurisé dans les propriétés du répertoire racine.

Remarque : Nous recommandons d'importer les fichiers de bibliothèque à partir d'un disque local.

Remarque : Pour plus d'informations sur les autorisations Windows requises pour différents rôles d'utilisateur, consultez la section Autorisations de Windows.

Utilisateurs et groupes

SCIEX OS utilise les noms d'utilisateurs et les mots de passe enregistrés dans la base de données du contrôleur de domaine primaire ou dans Active Directory. Les mots de passe sont gérés à l'aide des outils fournis avec Windows. Pour plus d'informations sur l'ajout et la configuration des personnes et des rôles, consultez la section Configurer l'accès au logiciel SCIEX OS.

Aide d'Active Directory

Lors de l'ajout d'utilisateurs dans l'espace de travail Configuration de SCIEX OS, spécifiez les comptes d'utilisateur au format UPN (User Principal Name). Les versions suivantes d'Active Directory sont prises en charge :

- Serveurs Windows 2012.

- Clients Windows 7, 64 bits
- Clients Windows 10, 64 bits

Système de fichiers Windows

Dans le logiciel SCIEX OS, les fichiers et les répertoires doivent être stockés sur une partition de disque dur formatée en NTFS, qui peut contrôler et auditer l'accès aux fichiers du logiciel SCIEX OS. Le système de fichiers FAT (File Allocation Table) ne peut pas contrôler ou auditer l'accès aux dossiers ou aux fichiers. Il n'est donc pas approprié dans un environnement sécurisé.

Autorisations des fichiers et des dossiers

Pour gérer la sécurité, l'administrateur du logiciel SCIEX OS doit avoir le droit de modifier les autorisations relatives au dossier `SCIEX OS Data`. L'accès doit être configuré par l'administrateur réseau.

Remarque : Réfléchissez au niveau d'accès au lecteur, au répertoire racine et aux dossiers de projets sur chaque ordinateur dont ont besoin les utilisateurs. Configurez le partage et les autorisations associées. Pour plus d'informations sur le partage de fichiers, consultez la documentation Windows.

Remarque : Pour éviter les problèmes d'autorisation, nous recommandons d'importer les fichiers de bibliothèque depuis un lecteur local.

Remarque : Pour plus d'informations sur les autorisations Windows requises pour différents rôles d'utilisateur, consultez la section Autorisations de Windows.

Pour plus d'informations sur les fichiers et les autorisations de dossier dans le logiciel SCIEX OS, consultez la section Contrôle d'accès à Analyst.

Audits du système

La fonction d'audit du système Windows peut être activée pour détecter les atteintes à la sécurité ou les intrusions dans le système. L'audit peut être défini de manière à enregistrer différents types d'événements liés au système. Par exemple, la fonction d'audit peut être activée pour enregistrer dans le journal d'événements toute tentative de connexion au système qui échoue ou réussit.

Registres d'événements

La visionneuse d'événements Windows enregistre les événements audités dans le registre de sécurité, le registre système ou le registre des applications.

Personnalisez les registres d'événements comme suit :

- Configurez une taille de journal d'événements adaptée.
- Activez l'écrasement automatique des anciens événements.
- Définissez les paramètres de sécurité Windows sur l'ordinateur.

Il est possible de mettre en place un processus d'examen et de stockage. Pour plus d'informations sur les paramètres de sécurité et les politiques relatives aux audits, consultez la documentation Windows.

Alertes Windows

Si un problème survient sur le système ou en lien avec l'utilisateur, configurez le réseau de façon à ce qu'il envoie un message automatique à la personne concernée telle que l'administrateur système sur le même ordinateur ou sur un autre.

- Sur l'ordinateur émetteur et sur l'ordinateur destinataire, démarrez le service Messenger dans le panneau de configuration des services Windows.
- Sur l'ordinateur émetteur, démarrez le service d'alerte dans le panneau de configuration des services Windows.

Pour plus d'informations sur la création d'un objet d'alerte, consultez la documentation Windows.

Octroi d'une licence électronique 3

Pour le logiciel SCIEX OS, les licences électroniques peuvent être de type blocage de nœud ou serveur.

Pour le logiciel Central Administrator Console (CAC), seules les licences à blocage de nœud sont prises en charge.

L'ID d'activation peut s'avérer nécessaire pour tout appel ultérieur de maintenance ou d'assistance. Pour accéder à l'ID d'activation de la licence avec blocage de nœud ou sur serveur :

- Dans l'espace de travail Configuration, cliquez sur **Licences** dans la fenêtre SCIEX OS.

Remarque : Veillez à bien renouveler la licence avant qu'elle n'arrive à expiration. La licence du logiciel CAC est une licence annuelle.

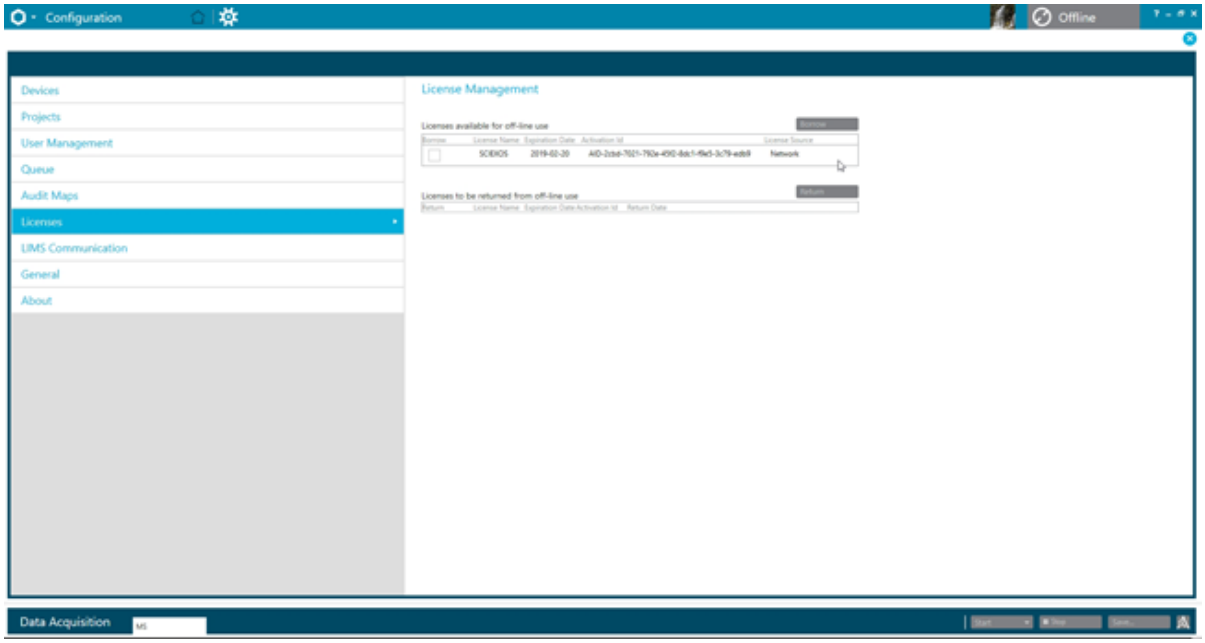
Emprunter une licence électronique sur serveur

Une licence est requise pour utiliser SCIEX OS. Avec des licences sur serveur, les utilisateurs qui veulent travailler hors ligne peuvent réserver une licence pendant 7 jours au maximum. Pendant cette période, la licence électronique empruntée est dédiée à l'ordinateur.

Remarque : Cette procédure n'est pas applicable pour le logiciel Central Administrator Console (CAC).

1. Ouvrez l'espace de travail Configuration.
2. Cliquez sur **Licences**.
   Le tableau Licences disponibles pour une utilisation hors ligne affiche toutes les licences pouvant être empruntées.

Illustration 3-1 : Gestion des licences : Emprunter une licence



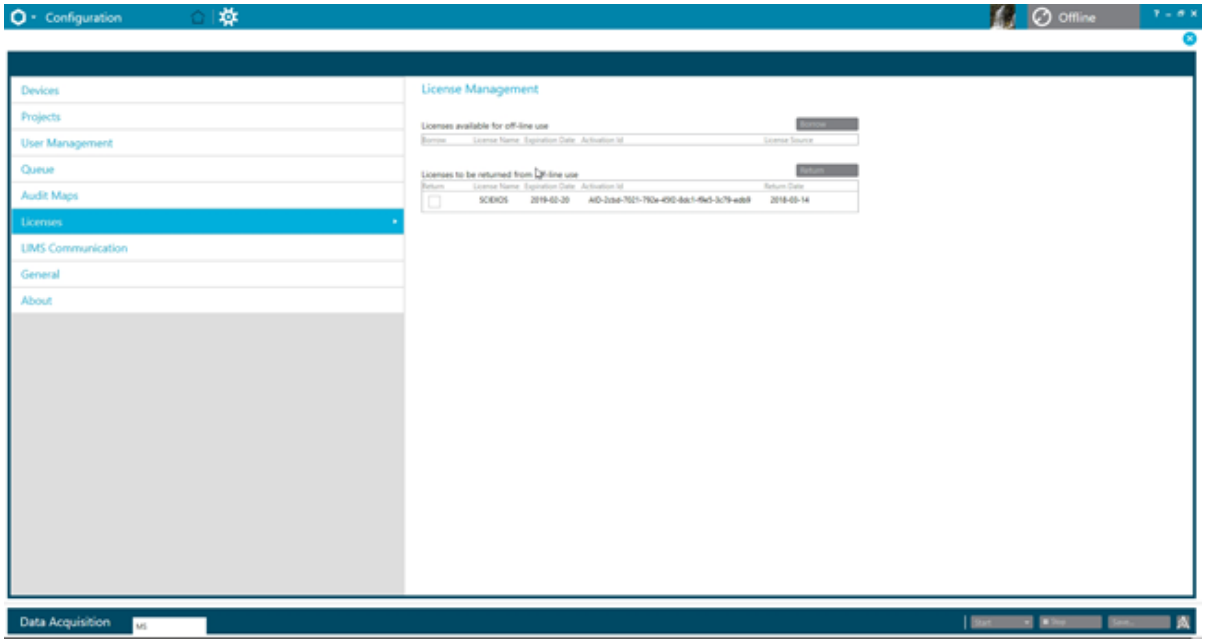
3. Sélectionnez la licence à emprunter, puis cliquez sur **Emprunter**.

Restituer une licence électronique sur serveur

Remarque : Cette procédure n'est pas applicable pour le logiciel Central Administrator Console (CAC).

1. Ouvrez l'espace de travail Configuration.
2. Cliquez sur **Licences**.
   Le tableau Licences à restituer après utilisation hors ligne présente toutes les licences qui peuvent être restituées (toutes les licences empruntées par cet ordinateur).

Illustration 3-2 : Gestion des licences : Restituer une licence



3. Sélectionnez la licence à restituer, puis cliquez sur **Restituer**.

Contrôle d'accès à Analyst 4

Cette section décrit comment contrôler l'accès au logiciel SCIEX OS. Pour contrôler l'accès au logiciel, l'administrateur effectue les tâches suivantes :

Remarque : Pour effectuer les tâches de cette section, l'utilisateur doit posséder des droits d'administrateur local sur le poste de travail où le logiciel est installé.

- Installez et configurez le logiciel SCIEX OS.
- Ajoutez et configurez les utilisateurs et les rôles.
- Configurez l'accès aux projets et aux fichiers du projet dans le répertoire racine.

Cette procédure fournit des instructions pour l'administration locale du logiciel SCIEX OS. Pour l'administration centralisée du logiciel SCIEX OS, consultez la section Central Administrator Console.

Remarque : Toute modification apportée à la configuration d'SCIEX OS prend effet après le redémarrage d'SCIEX OS.

Emplacement des informations de sécurité

Toutes les informations de sécurité sont stockées sur l'ordinateur local, dans le dossier `C:\ProgramData\SCIEX\Clearcore2.Acquisition`, dans un fichier nommé `Security.data`.

Flux de travail de la sécurité logicielle

Le logiciel SCIEX OS travaille avec les composants de sécurité, d'application et d'audit des événements système des Windows Administrative Tools.

Configurez la sécurité aux niveaux suivants :

- Authentification Windows : accès à l'ordinateur.
- Authentification Windows : accès aux fichiers et dossiers.
- Authentification du logiciel SCIEX OS : capacité à ouvrir SCIEX OS.
- Autorisation du logiciel SCIEX OS : accès à la fonctionnalité dans SCIEX OS.

Pour la liste des tâches de configuration de la sécurité, consultez le tableau Tableau 4-1. Pour les options de définition des différents niveaux de sécurité, consultez le tableau Tableau 4-2.

Tableau 4-1 : Flux de travail pour configurer la sécurité

Tâche	Procédure
Installer le logiciel SCIEX OS.	Consulter le document *Guide d'installation du logiciel SCIEX OS*.
Configurer l'accès au logiciel SCIEX OS.	Consulter la section Configurer l'accès au logiciel SCIEX OS.
Configurer Windows File Security et NTFS.	Consulter la section Configurer l'accès aux projets et aux fichiers de projet.

Tableau 4-2 : Options de configuration de la sécurité

Option	CFR 21 Part 11
Sécurité Windows	
Configurer les utilisateurs et les groupes (authentification).	Oui
Autoriser l'audit de Windows ainsi que l'audit des fichiers et des répertoires.	Oui
Configurer les autorisations sur les fichiers (autorisation).	Oui
Installation du logiciel SCIEX OS	
Installer le logiciel SCIEX OS.	Oui
Ouvrir la visionneuse d'événements pour inspecter l'installation.	Oui
Sécurité du logiciel	
Sélectionner le mode de sécurité.	Oui
Configurer les utilisateurs et les rôles dans le logiciel SCIEX OS.	Oui
Configurer la notification par courrier électronique.	Oui
Créer des modèles de cartes d'audit et configurer des cartes de registres d'audit de poste de travail et de projet.	Oui
Activer la fonction de somme de contrôle pour les fichiers `wiff`.	Oui
Tâches courantes	
Ajouter de nouveaux projets.	Oui

Installer le logiciel SCIEX OS

Avant d'installer le logiciel SCIEX OS, lisez ces documents disponibles sur le DVD d'installation du logiciel ou dans le package de téléchargement Web : *Guide d'installation du logiciel* et *Notes de version*. Veillez à bien comprendre la différence entre un ordinateur de traitement et un ordinateur d'acquisition, puis suivez la séquence d'installation qui convient.

Configuration système requise

Vous trouverez la configuration requise pour l'installation dans le document : *Guide d'installation du logiciel*.

Options d'audit préréglées

Pour une description des cartes d'audit installées, consultez la section Modèles de carte d'audit installés. Après l'installation, l'administrateur du logiciel SCIEX OS peut créer des cartes d'audit personnalisées et attribuer une autre carte d'audit dans l'espace de travail Configuration.

Configurer le mode de sécurité

Cette section décrit les options Mode sécurité sur la page Gestion des utilisateurs dans l'espace de travail Configuration.

Mode intégré : si l'utilisateur connecté à Windows est défini comme un utilisateur dans le logiciel, il a accès au logiciel SCIEX OS.

Mode mixte : les utilisateurs se connectent séparément à Windows et au logiciel. Il n'est pas nécessaire que les identifiants de connexion à Windows et à SCIEX OS CAC soient les mêmes. Utilisez ce mode pour autoriser un groupe d'utilisateurs à se connecter à Windows avec les mêmes identifiants, mais exigez que chaque utilisateur se connecte au logiciel avec des identifiants uniques. Ces identifiants uniques peuvent être affectés à un rôle donné de la même manière qu'en mode intégré.

Si le mode mixte est sélectionné, les fonctionnalités Verrouillage de l'écran et Déconnexion automatique sont prêtes à être utilisées.

Verrouillage de l'écran et Déconnexion automatique : pour des questions de sécurité, l'écran de l'ordinateur peut être paramétré pour se verrouiller après un certain temps d'inactivité. Il est également possible de définir une temporisation de déconnexion automatique afin que le logiciel se ferme après avoir été verrouillé pendant une durée définie. Les fonctions Verrouillage de l'écran et Déconnexion automatique sont disponibles en mode mixte uniquement.

Remarque : Lorsque l'écran se verrouille, l'acquisition et le traitement se poursuivent. Il n'y a pas de déconnexion automatique si un traitement est en cours ni si le tableau de résultats n'a pas été sauvegardé. Lorsque l'utilisateur est déconnecté de manière forcée, tout traitement s'arrête et les données qui n'ont pas été sauvegardées sont perdues. L'acquisition continues après la déconnexion de l'utilisateur, qu'elle soit automatique ou manuelle.

Notification de sécurité : le logiciel peut être configuré pour envoyer automatiquement une notification par e-mail après un nombre configurable d'échecs de connexion sur une durée configurable afin de signaler des tentatives d'accès au système par des utilisateurs non autorisés. Le nombre d'échecs de connexion peut être défini entre 3 et 7, et la durée entre 5 minutes et 24 heures.

Remarque : Pour les groupes de travail administrés par le logiciel Central Administrator Console (CAC), le mode de sécurité ne peut pas être géré avec SCIEX OS.

Sélectionner le mode de sécurité

1. Ouvrez l'espace de travail Configuration.
2. Cliquez sur **Gestion des utilisateurs**.
3. Cliquez sur l'onglet **Mode de sécurité**.
4. Sélectionnez **Mode intégré** ou **Mode mixte**. Consultez la section Configurer le mode de sécurité.
5. Cliquez sur **Enregistrer**.
   Une boîte de dialogue de confirmation apparaît.
6. Cliquez sur **OK**.

Configurer les options de sécurité du poste de travail (Mixed Mode)

Procédures préalables
• Définissez le mode de sécurité sur Mixed Mode. Consultez la section Configurer le mode de sécurité.

Si le mode Mixed est sélectionné, les fonctionnalités Screen Lock et Auto Logoff peuvent être configurées.

1. Ouvrez l'espace de travail Configuration.
2. Cliquez sur **Gestion des utilisateurs**.
3. Ouvrez l'onglet Mode sécurité.
4. Respectez les étapes suivantes pour configurer la fonction Screen Lock :
   a. Sélectionnez **Verrouillage de l'écran**.
   b. Dans le champ **Attente**, spécifiez une durée en minutes.
      Si le poste de travail reste inactif pendant cette durée, il est automatiquement verrouillé. L'utilisateur connecté peut déverrouiller le poste de travail en saisissant les identifiants corrects, ou l'Administrateur peut déconnecter l'utilisateur.
5. Respectez les étapes suivantes pour configurer la fonction Auto Logoff :
   a. Sélectionnez **Déconnexion automatique**.
   b. Dans le champ **Attente**, spécifiez une durée en minutes. Si le poste de travail reste verrouillé pendant cette durée, automatiquement ou manuellement, l'utilisateur connecté actuellement est déconnecté. Tout traitement prend fin. Toutefois, l'acquisition continue.
6. Cliquez sur **Enregistrer**.

Une boîte de dialogue de confirmation apparaît.

7. Cliquez sur **OK**.

Configurer une notification par e-mail (Mixed Mode)

Procédures préalables
• Définissez le mode de sécurité sur Mixed Mode. Consultez la section Configurer le mode de sécurité.

Le logiciel peut être configuré pour envoyer un e-mail après un nombre configurable d'erreurs de connexion sur une durée donnée. Le nombre d'échecs de connexion peut être défini entre 3 et 7, et la durée entre 5 minutes et 24 heures.

L'ordinateur avec le logiciel installé doit pouvoir communiquer avec un serveur SMTP avec un port ouvert.

1. Ouvrez l'espace de travail Configuration.
2. Cliquez sur **Gestion des utilisateurs**.
3. Ouvrez l'onglet Mode sécurité.
4. Cochez la case **Envoyer les messages par e-mail après** puis spécifiez le nombre d'erreurs de connexion et la durée en minutes pour générer une notification par e-mail.

   Conseil ! Pour désactiver la notification, décochez la case **Envoyer les messages par e-mail après**.

5. Dans le champ **Serveur SMTP**, inscrivez le nom du serveur SMTP.

   Remarque : Le compte SMTP envoie un courrier électronique au serveur de courrier électronique. Le serveur SMTP est défini dans l'application de messagerie électronique de l'entreprise.

6. Dans le champ **Numéro de port**, inscrivez le numéro du port ouvert.
   Cliquez sur **Appliquer la valeur par défaut** pour insérer le numéro de port par défaut, 25.
7. Dans le champ **À**, saisissez l'adresse électronique à laquelle le message doit être envoyé. Par exemple : username@domain.com.
8. Dans le champ **De**, saisissez l'adresse électronique à afficher dans le champ **De** du message.
9. Dans le champ **Objet**, inscrivez le sujet du message.
10. Dans le champ **Message**, saisissez le texte à inclure dans le corps du message.
11. Cliquez sur **Enregistrer**.
    Une boîte de dialogue de confirmation apparaît.
12. Cliquez sur **OK**.

13. Pour vérifier la configuration, cliquez sur **Envoyer le message de test**.

Configurer l'accès au logiciel SCIEX OS

Avant de configurer la sécurité, procédez comme suit :

- Supprimez tous les utilisateurs et les groupes d'utilisateurs inutiles tels que le multiplicateur, l'utilisateur expérimenté et l'opérateur de sauvegarde à partir de l'ordinateur local et du réseau.

  Remarque : Chaque ordinateur SCIEX est configuré avec un compte de niveau administrateur local, **abservice**. Le personnel d'intervention et l'assistance technique SCIEX utilisent ce compte pour installer, entretenir et réparer le système. Ne pas supprimer ni désactiver ce compte. Si ce compte est supprimé ou désactivé, préparer un autre moyen d'accéder à SCIEX et le communiquer au technicien de service local.

- Ajoutez les groupes d'utilisateur contenant les groupes auxquels seront attribuées des tâches non administratives.
- Configurez les autorisations du système.
- Créez des procédures adéquates et des politiques de compte pour les utilisateurs dans la politique du groupe.

Consultez la documentation Windows pour plus d'informations sur les points suivants :

- Utilisateurs, groupes et utilisateurs d'Active Directory
- Politiques relatives aux mots de passe et au verrouillage de compte pour les comptes utilisateur.
- Politique des droits des utilisateurs

Lorsque les utilisateurs travaillent dans un environnement Active Directory, les paramètres de la politique du groupe Active Directory ont une incidence sur la sécurité de l'ordinateur. Discutez des politiques de groupe avec l'administrateur Active Directory dans le cadre d'un déploiement global du logiciel SCIEX OS.

Autorisations SCIEX OS

Illustration 4-1 : Page User Management

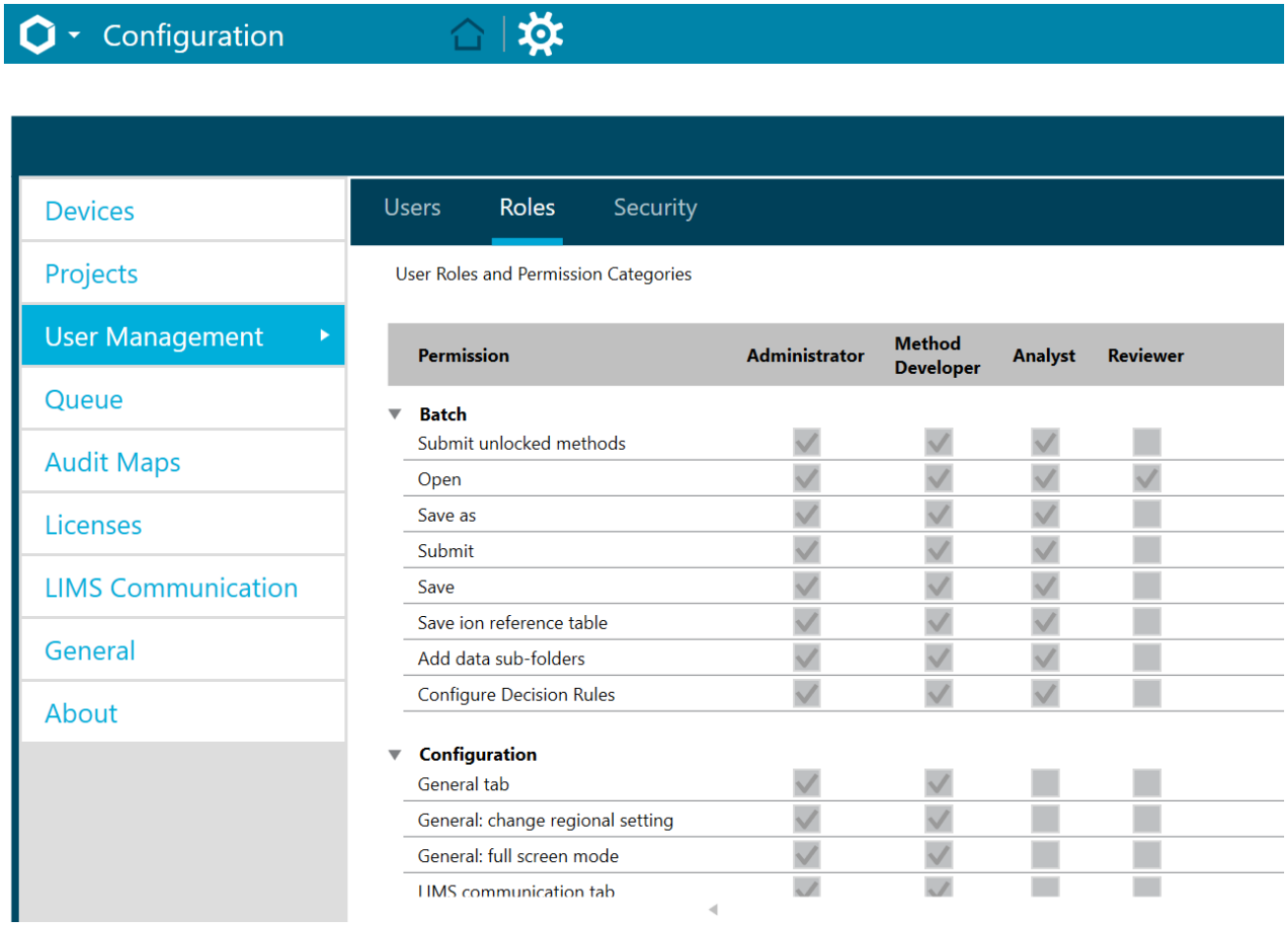


Tableau 4-3 : Autorisations

Autorisation	Description
Lot	
Envoyer les méthodes déverrouillées	Permet aux utilisateurs de soumettre des lots contenant des méthodes déverrouillées.
Ouvrir	Permet aux utilisateurs d'ouvrir des lots.
Enregistrer sous	Permet aux utilisateurs d'enregistrer des lots sous un nouveau nom.
Envoyer	Permet aux utilisateurs de soumettre des lots.
Enregistrer	Permet aux utilisateurs d'enregistrer un lot et d'écraser le contenu existant.
Enregistrer le tableau de référence d'ions	Permet aux utilisateurs de modifier le tableau de référence des ions.

Tableau 4-3 : Autorisations (suite)

Autorisation	Description
Ajouter des sous-dossiers de données	Permet aux utilisateurs de créer des sous-dossiers pour stocker les données.
Configurer les règles de décision	Permet aux utilisateurs d'ajouter et de modifier des règles de décision.
Configuration	
Onglet Général	Permet aux utilisateurs d'ouvrir la page Général dans l'espace de travail Configuration.
Général : modifier le paramètre régional	Permet aux utilisateurs d'appliquer les paramètres régionaux actifs du système au logiciel SCIEX OS.
Général : mode plein écran	Permet aux utilisateurs d'activer ou de désactiver le mode plein écran.
Général : arrêter les services Windows	Permet aux utilisateurs d'activer ou de désactiver l'option **Paramètres Windows**.
Onglet Communication LIMS	Permet aux utilisateurs d'ouvrir la page Communication LIMS dans l'espace de travail Configuration.
Onglet Cartes d'audit	Permet aux utilisateurs d'ouvrir la page Cartes d'audit dans l'espace de travail Configuration.
Onglet File d'attente	Permet aux utilisateurs d'ouvrir la page File d'attente dans l'espace de travail Configuration.
File d'attente : période d'inactivité de l'instrument	Permet aux utilisateurs de définir le temps d'inactivité de l'instrument.
File d'attente : nombre max. d'échantillons acquis	Permet aux utilisateurs de définir le nombre maximum autorisé d'échantillons acquis.
File d'attente : autres paramètres de file d'attente	Permet aux utilisateurs de configurer d'autres paramètres de la file attente.
Onglet Projets	Permet aux utilisateurs d'ouvrir la page Projets dans l'espace de travail Configuration.
Projets : créer un projet	Permet aux utilisateurs de créer des projets.
Projets : appliquer un modèle de carte d'audit à un projet	Permet aux utilisateurs d'appliquer une carte d'audit à un projet.
Projets : créer le répertoire racine	Permet aux utilisateurs de créer un répertoire racine pour stocker les projets.
Projets : définir le répertoire racine actuel	Permet aux utilisateurs de modifier le répertoire racine d'un projet.

Tableau 4-3 : Autorisations (suite)

Autorisation	Description
Projets : spécifier les identifiants réseau	Permet aux utilisateurs de spécifier le compte réseau sécurisé (SNA) à utiliser lors de l'acquisition réseau si l'utilisateur connecté n'a pas accès à la ressource réseau.
Projets : activer l'écriture de somme de contrôle pour la création de données wiff	Permet aux utilisateurs de configurer le logiciel pour écrire les sommes de contrôle dans les fichiers de données `wiff`.
Projets : effacer le répertoire racine	Permet aux utilisateurs de supprimer un répertoire racine de la liste.
Onglet Appareils	Permet aux utilisateurs d'ouvrir la page Appareils dans l'espace de travail Configuration.
Onglet Gestion des utilisateurs	Permet aux utilisateurs d'ouvrir la page Gestion des utilisateurs dans l'espace de travail Configuration.
Forcer la déconnexion de l'utilisateur	Permet aux utilisateurs de forcer la déconnexion de l'utilisateur connecté au logiciel SCIEX OS.
Onglet CAC [1]	Permet aux utilisateurs d'ouvrir la page CAC dans l'espace de travail Configuration.
Onglet Modèles d'impression	Permet aux utilisateurs d'ouvrir l'onglet Modèles d'impression dans l'espace de travail Configuration.
Modèles d'impression : Créer et modifier des modèles d'impression	Permet aux utilisateurs de créer ou de modifier des modèles d'impression.
Modèles d'impression : Définir le modèle d'impression par défaut	Permet aux utilisateurs de définir le modèle d'impression actuel comme modèle par défaut du projet actif.
Modèles d'impression : Appliquer le modèle actuel à tous les projets du répertoire racine	Permet aux utilisateurs d'ajouter le modèle d'impression à la liste des modèles d'impression disponibles pour les projets sélectionnés dans un répertoire racine sélectionné.
Registre d'événements	
Accéder à l'espace de travail Registre d'événements	Permet aux utilisateurs d'ouvrir l'espace de travail Registre d'événements.
Archiver le registre	Permet aux utilisateurs d'archiver les registres dans l'espace de travail Registre d'événements.
Trace d'audit	

[1] Dans la version 3.1, l'autorisation **Activer Central Administration** a été renommée en **CAC**. La page CAC dans l'espace de travail Configuration permet de configurer l'administration centrale du logiciel SCIEX OS.

Tableau 4-3 : Autorisations (suite)

Autorisation	Description
Accéder à l’espace de travail Trace d'audit	Permet aux utilisateurs d'ouvrir l'espace de travail Trace d'audit.
Afficher la carte d'audit active	Permet aux utilisateurs d'afficher la carte d'audit active pour un poste de travail ou un projet dans l'espace de travail Audit Trail.
Imprimer/exporter la trace d'audit	Permet aux utilisateurs d'imprimer ou d'exporter le registre d'audit.
Volet Acquisition des données	
Démarrage	Permet aux utilisateurs de commencer l'acquisition dans le volet Acquisition des données.
Arrêter	Permet aux utilisateurs d'arrêter l'acquisition dans le volet Acquisition des données.
Enregistrer	Permet aux utilisateurs d’enregistrer les données acquises sous un autre nom de fichier dans le volet Acquisition des données.
Méthodes MS et LC	
Accéder à l’espace de travail Méthode	Permet aux utilisateurs d’ouvrir les espaces de travail Méthode MS et Méthode LC.
Nouveau	Permet aux utilisateurs de créer des méthodes MS et LC.
Ouvrir	Permet aux utilisateurs d'ouvrir des méthodes MS et LC.
Enregistrer	Permet aux utilisateurs d'enregistrer une méthode et d’écraser le contenu existant.
Enregistrer sous	Permet aux utilisateurs d'enregistrer des méthodes sous un nouveau nom.
Verrouiller/déverrouiller la méthode	Permet aux utilisateurs de verrouiller les méthodes pour empêcher leur modification et de les déverrouiller.
File d'attente	
Gérer	Permet aux utilisateurs d'ouvrir l'espace de travail File d'attente.
Démarrer/Arrêter	Permet aux utilisateurs de démarrer ou d'arrêter la file d'attente.
Imprimer	Permet aux utilisateurs d’imprimer la file d’attente.
Modifier l'échantillon	Permet aux utilisateurs de modifier le nom ou le fichier de données d’un échantillon.
Bibliothèque	

Tableau 4-3 : Autorisations (suite)

Autorisation	Description
Accéder à l'espace de travail Bibliothèque	Permet aux utilisateurs d'ouvrir l'espace de travail Bibliothèque. Non applicable au flux de travail Quantitation.
Réglage MS	
Accéder à l'espace de travail Réglage MS	Permet aux utilisateurs d'ouvrir l'espace de travail Réglage MS.
Réglage MS avancé	Systèmes X500 QTOF et ZenoTOF 7600 : permet aux utilisateurs d'accéder aux options de réglage avancées, comme **Optimisation du détecteur**, **Réglage TOF positif**, **Réglage TOF négatif**, **Réglage d'unité Q1 positif**, **Réglage d'unité Q1 négatif**, **Réglage haut de Q1 positif** et **Réglage haut de Q1 négatif**.
Dépannage avancé	Permet aux utilisateurs d'ouvrir la boîte de dialogue Dépannage avancé.
Vérification d'état rapide	Systèmes X500 QTOF et ZenoTOF 7600 : permet aux utilisateurs d'effectuer les opérations **Vérification d'état rapide positif** et **Vérification d'état rapide négatif**.
Restaurer les données de l'instrument	Permet aux utilisateurs de restaurer les paramètres d'ajustement sauvegardés.
Explorateur	
Accéder à l'espace de travail Explorateur	Permet aux utilisateurs d'ouvrir l'espace de travail Explorateur.
Exporter	Permet aux utilisateurs d'exporter des données depuis l'espace de travail Explorateur.
Imprimer	Permet aux utilisateurs d'imprimer des données dans l'espace de travail Explorateur.
Options	Permet aux utilisateurs de modifier les options de l'espace de travail Explorateur.
Réétalonner	Permet aux utilisateurs de réétalonner les échantillons et les spectres dans l'espace de travail Explorateur. Non applicable au flux de travail Quantitation.
Analytics	
Nouveaux résultats	Permet aux utilisateurs de créer des tableaux de résultats.
Créer une méthode de traitement	Permet aux utilisateurs de créer des méthodes de traitement.
Modifier la méthode de traitement	Permet aux utilisateurs de modifier les méthodes de traitement.

Tableau 4-3 : Autorisations (suite)

Autorisation	Description
Autoriser l'exportation et la création d'un rapport du tableau de résultats déverrouillé	Permet aux utilisateurs d’exporter ou de générer un rapport à partir d’un tableau de résultats ou d’un tableau de statistiques si le tableau de résultats n’est pas verrouillé.
Enregistrer les résultats pour le lot d’automatisation	Permet d’enregistrer les tableaux de résultats créés automatiquement dans l’espace de travail Lot. Cette autorisation est requise pour le traitement automatique pendant l’acquisition.
Modifier l'algorithme d'intégration de la méthode de quantification par défaut	Permet aux utilisateurs de modifier l'algorithme d'intégration dans les paramètres par défaut du projet.
Modifier les paramètres d'intégration de la méthode de quantification par défaut	Permet aux utilisateurs de modifier les paramètres d'intégration dans les paramètres par défaut du projet.
Activer l'avertissement de pic modifié du projet	Permet aux utilisateurs d'activer la propriété d'avertissement de modification de pic dans un projet.
Ajouter des échantillons	Permet aux utilisateurs d'ajouter des échantillons dans un tableau de résultats.
Supprimer les échantillons sélectionnés	Permet aux utilisateurs de supprimer des échantillons d'un tableau de résultats.
Exporter, importer ou supprimer un étalonnage externe	Permet aux utilisateurs d'exporter, importer ou supprimer des étalonnages externes.
Modifier le nom de l'échantillon	Permet aux utilisateurs de modifier le nom de l'échantillon dans le tableau de résultats.
Modifier le type d'échantillon	Permet aux utilisateurs de modifier le type d'échantillon dans le tableau de résultats. Les types d'échantillon autorisés sont Standard, Quality Control (QC) et Unknown.
Modifier l'ID d'échantillon	Permet aux utilisateurs de modifier l’ID de l'échantillon dans le tableau de résultats.
Modifier la concentration réelle	Permet aux utilisateurs de modifier la concentration réelle des échantillons standard et QC dans le tableau de résultats.
Modifier le facteur de dilution	Permet aux utilisateurs de modifier le facteur de dilution dans le tableau de résultats.

Tableau 4-3 : Autorisations (suite)

Autorisation	Description
Modifier les champs de commentaires	Permet aux utilisateurs de modifier les champs de commentaire suivants : • **Commentaire de composant** • **Commentaire d'IS** • **Commentaire de pic d'IS** • **Commentaire de pic** • **Commentaire d'échantillon**
Activer l'intégration manuelle	Permet aux utilisateurs d'effectuer l'intégration manuelle.
Définir le pic comme non trouvé	Permet aux utilisateurs de régler un pic sur **Non trouvé**.
Inclure un pic dans le tableau de résultats ou l'en exclure	Permet aux utilisateurs d'inclure des pics dans le tableau de résultats ou de les exclure de ce dernier.
Options de régression	Permet aux utilisateurs de modifier les options de régression dans le volet Courbe d'étalonnage.
Modifier les paramètres d'intégration du tableau de résultats pour un chromatogramme	Permet aux utilisateurs de modifier les paramètres d'intégration d'un chromatogramme dans le volet Examen des pics.
Modifier la méthode de quantification du composant du tableau de résultats	Permet aux utilisateurs de sélectionner une autre méthode de traitement pour un composant dans le volet Examen des pics avec l'option **Mettre à jour la méthode de traitement du composant**.
Créer des paramètres de tracé métrique	Permet aux utilisateurs de créer des tracés métriques et de modifier les paramètres.
Ajouter des colonnes personnalisées	Permet aux utilisateurs d'ajouter des colonnes personnalisées dans un tableau de résultats.
Définir le format du titre de l'examen des pics	Permet aux utilisateurs de modifier le titre de l'examen des pics.
Supprimer la colonne personnalisée	Permet aux utilisateurs de supprimer des colonnes personnalisées d'un tableau de résultats.
Paramètres d'affichage du tableau de résultats	Permet aux utilisateurs de personnaliser les colonnes affichées dans le tableau de résultats.
Verrouiller le tableau de résultats	Permet aux utilisateurs de verrouiller un tableau de résultats pour éviter qu'il soit modifié.

Tableau 4-3 : Autorisations (suite)

Autorisation	Description
Déverrouiller le tableau de résultats	Permet aux utilisateurs de déverrouiller un tableau de résultats et de le modifier.
Marquer le fichier de résultats comme révisé et l'enregistrer	Permet aux utilisateurs de marquer un tableau de résultats comme examiné et de l'enregistrer.
Modifier le modèle de rapport	Permet aux utilisateurs de modifier des modèles de rapport.
Transférer les résultats à LIMS	Permet aux utilisateurs de charger des résultats dans un système LIMS (Laboratory Information Management System).
Modifier la colonne de code-barres	Permet aux utilisateurs de modifier la colonne **Code-barres** dans un tableau de résultats.
Modifier l'affectation d'échantillon de comparaison	Permet aux utilisateurs de modifier l'échantillon de comparaison spécifié dans la colonne **Comparaison** du tableau de résultats.
Ajouter les spectres MSMS à la bibliothèque	Permet aux utilisateurs d'ajouter des spectres MS/MS dans une bibliothèque. Non applicable au flux de travail Quantitation.
Paramètres par défaut du projet	Permet aux utilisateurs de modifier les paramètres de traitement quantitatif et qualitatif par défaut du projet.
Créer un rapport dans tous les formats	Permet aux utilisateurs de créer des rapports dans tous les formats. Les utilisateurs ne possédant pas cette autorisation ne peuvent que générer des rapports au format PDF.
Modifier les paramètres du critère de marquage	Permet aux utilisateurs de modifier les paramètres de marquage d'une méthode de traitement.
Modification du paramètre de suppression automatique des données aberrantes	Permet aux utilisateurs de modifier les paramètres de suppression automatique des données aberrantes.
Activer la suppression automatique des données aberrantes	Permet aux utilisateurs de modifier la méthode de traitement pour activer la fonction de suppression automatique des données aberrantes.
Mettre à jour la méthode de traitement via FF/LS	Permet aux utilisateurs d'utiliser Formula Finder et Library Search pour mettre à jour des méthodes de traitement. Non applicable au flux de travail Quantitation.
Mettre à jour les résultats via FF/LS	Permet aux utilisateurs d'utiliser Formula Finder et Library Search pour mettre à jour des résultats. Non applicable au flux de travail Quantitation.

Tableau 4-3 : Autorisations (suite)

Autorisation	Description
Activer la fonction de regroupement par adduits	Permet aux utilisateurs de mettre à jour la méthode de traitement pour utiliser la fonction de regroupement par adduits.
Rechercher des fichiers	Permet aux utilisateurs de naviguer hors du dossier de données local.
Activer l'ajout de standards	Permet aux utilisateurs de mettre à jour la méthode de traitement pour activer la fonction d'ajout de standard.
Définir la règle de pourcentage d'intégration manuelle	Permet aux utilisateurs de modifier le paramètre **Intégration manuelle %**.
Modifier le poids/volume	Permet à l'utilisateur de modifier le champ **Poids/Volume**.

À propos des utilisateurs et des rôles

Dans le logiciel SCIEX OS, l'administrateur peut ajouter des utilisateurs et des groupes Windows à la base de données de gestion des utilisateurs. Pour accéder au logiciel, les utilisateurs doivent être définis dans la base de données de gestion des utilisateurs ou être membres d'un groupe dans cette base de données.

Les utilisateurs peuvent être assignés à un ou plusieurs des rôles prédéfinis affichés dans le tableau suivant, ou à des rôles personnalisés le cas échéant. Les fonctions auxquels un utilisateur a accès dépendent des rôles. Les rôles prédéfinis ne peuvent pas être supprimés et leurs autorisations ne sont pas modifiables.

Remarque : Dans les groupes de travail administrés par le logiciel Central Administrator Console (CAC), les pages Gestion des utilisateurs sont en lecture seule.

Tableau 4-4 : Rôles prédéfinis

Rôle	Tâches habituelles
Administrateur	• Gère le système • Configure la sécurité
Développeur de méthode	• Crée des méthodes • Exécute des lots • Analyse les données à utiliser par l'utilisateur
Analyst	• Exécute des lots • Analyse les données à utiliser par l'utilisateur

Tableau 4-4 : Rôles prédéfinis (suite)

Rôle	Tâches habituelles
Examinateur	• Examine les données • Examine les registres d'audit • Examine les résultats de quantification

Tableau 4-5 : Autorisations prédéfinies

Autorisation	Administrateur	Développeur de méthode	Analyst	Examinateur
Lot				
Envoyer les méthodes déverrouillées	✓	✓	✓	×
Ouvrir	✓	✓	✓	✓
Enregistrer sous	✓	✓	✓	×
Envoyer	✓	✓	✓	×
Enregistrer	✓	✓	✓	×
Enregistrer le tableau de référence d'ions	✓	✓	✓	×
Ajouter des sous-dossiers de données	✓	✓	✓	×
Configurer les règles de décision	✓	✓	✓	×
Configuration				
Onglet Général	✓	✓	×	×
Général : modifier le paramètre régional	✓	✓	×	×
Général : mode plein écran	✓	✓	×	×
Général : arrêter les services Windows	✓	×	×	×
Onglet Communication LIMS	✓	✓	×	×
Onglet Cartes d'audit	✓	×	×	×
Onglet File d'attente	✓	✓	✓	✓

Tableau 4-5 : Autorisations prédéfinies (suite)

Autorisation	Administrateur	Développeur de méthode	Analyst	Examinateur
File d'attente : période d'inactivité de l'instrument	✓	✓	×	×
File d'attente : nombre max. d'échantillons acquis	✓	✓	×	×
File d'attente : autres paramètres de file d'attente	✓	✓	×	×
Onglet Projets	✓	✓	✓	✓
Projets : créer un projet	✓	✓	✓	×
Projets : appliquer un modèle de carte d'audit à un projet	✓	×	×	×
Projets : créer le répertoire racine	✓	×	×	×
Projets : définir le répertoire racine actuel	✓	×	×	×
Projets : spécifier les identifiants réseau	✓	×	×	×
Projets : activer l'écriture de somme de contrôle pour la création de données wiff	✓	×	×	×
Projets : effacer le répertoire racine	✓	×	×	×
Onglet Appareils	✓	✓	✓	×
Onglet Gestion des utilisateurs	✓	×	×	×
Forcer la déconnexion de l'utilisateur	✓	×	×	×
Onglet CAC[1]	✓	×	×	×

Tableau 4-5 : Autorisations prédéfinies (suite)

Autorisation	Administrateur	Développeur de méthode	Analyst	Examinateur
Onglet Modèles d'impression	✓	✓	×	×
Modèles d'impression : Créer et modifier des modèles d'impression	✓	✓	×	×
Modèles d'impression : Définir le modèle d'impression par défaut	✓	✓	×	×
Modèles d'impression : Appliquer le modèle actuel à tous les projets du répertoire racine	✓	×	×	×
Registre d'événements				
Accéder à l'espace de travail Registre d'événements	✓	✓	✓	✓
Registre d'archive	✓	✓	✓	✓
Trace d'audit				
Accéder à l'espace de travail Trace d'audit	✓	✓	✓	✓
Afficher la carte d'audit active	✓	✓	✓	✓
Imprimer/exporter la trace d'audit	✓	✓	✓	✓
Volet Acquisition des données				
Démarrage	✓	✓	✓	×
Arrêter	✓	✓	✓	×

[1] Dans la version 3.1, l'autorisation **Activer Central Administration** a été renommée en **CAC**. La page CAC dans l'espace de travail Configuration permet de configurer l'administration centrale du logiciel SCIEX OS.

Tableau 4-5 : Autorisations prédéfinies (suite)

Autorisation	Administrateur	Développeur de méthode	Analyst	Examinateur
Enregistrer	✓	✓	✓	×
Méthodes MS et LC				
Accéder à l'espace de travail Méthode	✓	✓	✓	✓
Nouveau	✓	✓	×	×
Ouvrir	✓	✓	✓	✓
Enregistrer	✓	✓	×	×
Enregistrer sous	✓	✓	×	×
Verrouiller/ déverrouiller la méthode	✓	✓	×	×
File d'attente				
Gérer	✓	✓	✓	×
Démarrer/Arrêter	✓	✓	✓	×
Imprimer	✓	✓	✓	✓
Modifier l'échantillon	✓	✓	×	×
Bibliothèque				
Accéder à l'espace de travail Bibliothèque	✓	✓	✓	✓
Réglage MS				
Accéder à l'espace de travail Réglage MS	✓	✓	✓	×
Réglage MS avancé	✓	✓	×	×
Dépannage avancé	✓	✓	×	×
Vérification d'état rapide	✓	✓	✓	×
Restaurer les données de l'instrument	✓	✓	×	×
Explorateur				

Tableau 4-5 : Autorisations prédéfinies (suite)

Autorisation	Administrateur	Développeur de méthode	Analyst	Examinateur
Accéder à l'espace de travail Explorateur	✓	✓	✓	✓
Exporter	✓	✓	✓	×
Imprimer	✓	✓	✓	×
Options	✓	✓	✓	×
Réétalonner	✓	✓	×	×
Analytics				
Nouveaux résultats	✓	✓	✓	×
Créer une méthode de traitement	✓	✓	✓	×
Modifier la méthode de traitement	✓	✓	×	×
Autoriser l'exportation et la création d'un rapport du tableau de résultats déverrouillé	✓	×	×	×
Enregistrer les résultats pour le lot d’automatisation	✓	✓	✓	×
Modifier l'algorithme d'intégration de la méthode de quantification par défaut	✓	✓	×	×
Modifier les paramètres d'intégration de la méthode de quantification par défaut	✓	✓	×	×
Activer l'avertissement de pic modifié du projet	✓	×	×	×
Ajouter des échantillons	✓	✓	✓	×

Tableau 4-5 : Autorisations prédéfinies (suite)

Autorisation	Administrateur	Développeur de méthode	Analyst	Examinateur
Supprimer les échantillons sélectionnés	✓	✓	✓	×
Exporter, importer ou supprimer un étalonnage externe	✓	✓	✓	×
Modifier le nom de l'échantillon	✓	✓	✓	×
Modifier le type d'échantillon	✓	✓	✓	×
Modifier l'ID d'échantillon	✓	✓	✓	×
Modifier la concentration réelle	✓	✓	✓	×
Modifier le facteur de dilution	✓	✓	✓	×
Modifier les champs de commentaires	✓	✓	✓	×
Activer l'intégration manuelle	✓	✓	✓	×
Définir le pic comme non trouvé	✓	✓	✓	×
Inclure un pic dans le tableau de résultats ou l’en exclure	✓	✓	✓	×
Options de régression	✓	✓	✓	×
Modifier les paramètres d'intégration du tableau de résultats pour un chromatogramme	✓	✓	✓	×
Modifier la méthode de quantification du composant du tableau de résultats	✓	✓	✓	×

Tableau 4-5 : Autorisations prédéfinies (suite)

Autorisation	Administrateur	Développeur de méthode	Analyst	Examinateur
Créer des paramètres de tracé métrique	✓	✓	✓	✓
Ajouter des colonnes personnalisées	✓	✓	✓	×
Définir le format du titre de l'examen des pics	✓	×	×	×
Supprimer la colonne personnalisée	✓	✓	×	×
Paramètres d'affichage du tableau de résultats	✓	✓	✓	✓
Verrouiller le tableau de résultats	✓	✓	✓	✓
Déverrouiller le tableau de résultats	✓	×	×	×
Marquer le fichier de résultats comme révisé et l'enregistrer	✓	×	×	✓
Modifier le modèle de rapport	✓	✓	×	×
Transférer les résultats à LIMS	✓	✓	✓	×
Modifier la colonne de code-barres	✓	✓	×	×
Modifier l'affectation d'échantillon de comparaison	✓	✓	×	×
Ajouter les spectres MSMS à la bibliothèque	✓	✓	×	×
Paramètres par défaut du projet	✓	✓	×	×
Créer un rapport dans tous les formats	✓	✓	✓	✓

Tableau 4-5 : Autorisations prédéfinies (suite)

Autorisation	Administrateur	Développeur de méthode	Analyst	Examinateur
Modifier les paramètres du critère de marquage	✓	✓	✓	×
Modification du paramètre de suppression automatique des données aberrantes	✓	✓	×	×
Activer la suppression automatique des données aberrantes	✓	✓	✓	×
Mettre à jour la méthode de traitement via FF/LS	✓	✓	×	×
Mettre à jour les résultats via FF/LS	✓	✓	×	×
Activer la fonction de regroupement par adduits	✓	✓	×	×
Rechercher des fichiers	✓	✓	✓	✓
Activer l'ajout de standards	✓	✓	✓	×
Définir la règle de pourcentage d'intégration manuelle	✓	×	×	×
Modifier le poids/ volume	✓	✓	✓	×

Gérer les utilisateurs

Ajouter un utilisateur ou un groupe

1. Ouvrez l'espace de travail Configuration.
2. Ouvrez la page Gestion des utilisateurs.
3. Ouvrez l'onglet Utilisateurs.

4. Cliquez sur **Ajouter un utilisateur** ().
   La boîte de dialogue Sélectionner un utilisateur ou un groupe s’ouvre.
5. Saisissez le nom d'un utilisateur ou d'un groupe, puis cliquez sur **OK**.

   Conseil ! Pour des informations sur la boîte de dialogue Sélectionner un utilisateur ou un groupe et son utilisation, appuyez sur **F1**.
6. Pour que l'utilisateur soit actif, vérifiez que la case **Utilisateur ou groupe actif** soit bien cochée.
7. Dans la section **Rôles**, sélectionnez un ou plusieurs rôles, puis cliquez sur **Enregistrer**.

Désactiver des utilisateurs ou des groupes

1. Ouvrez l'espace de travail Configuration.
2. Ouvrez la page Gestion des utilisateurs.
3. Ouvrez l’onglet Utilisateurs.
4. Dans la liste **Nom d’utilisateur ou groupe**, sélectionnez l'utilisateur ou le groupe à désactiver.
5. Décochez la case **Utilisateur ou groupe actif**.
   Le logiciel demande votre confirmation.
6. Cliquez sur **Oui**.

Supprimer des utilisateurs ou des groupes

Utilisez cette procédure pour supprimer un utilisateur ou un groupe du logiciel. Si un utilisateur ou un groupe est supprimé de Windows, il doit l'être également du logiciel SCIEX OS.

1. Ouvrez l'espace de travail Configuration.
2. Ouvrez la page Gestion des utilisateurs.
3. Ouvrez l’onglet Utilisateurs.
4. Dans la liste **Nom d’utilisateur ou groupe**, sélectionnez l'utilisateur ou le groupe à supprimer.
5. Cliquez sur **Supprimer**.
   Le logiciel demande votre confirmation.
6. Cliquez sur **OK**.

Gérer les rôles

Modifier les rôles attribués à un utilisateur ou à un groupe

Utilisez cette procédure pour attribuer de nouveaux rôles à un utilisateur ou à un groupe, ou pour supprimer les attributions de rôles existantes.

1. Ouvrez l'espace de travail Configuration.
2. Ouvrez la page Gestion des utilisateurs.
3. Ouvrez l’onglet Utilisateurs.
4. Dans le champ **Nom d’utilisateur ou groupe**, sélectionnez l'utilisateur ou le groupe à modifier.
5. Sélectionnez les rôles à attribuer à l'utilisateur ou au groupe et effacez les rôles à supprimer.
6. Cliquez sur **Enregistrer**.

Créer un rôle personnalisé

1. Ouvrez l'espace de travail Configuration.
2. Ouvrez la page Gestion des utilisateurs.
3. Ouvrez l’onglet Rôles.
4. Cliquez sur **Ajouter un rôle** ().
   La boîte de dialogue Dupliquer un rôle utilisateur s’ouvre.
5. Dans le champ **Rôle utilisateur existant**, sélectionnez le rôle à utiliser comme modèle pour le nouveau rôle.
6. Entrez un nom et une description pour le rôle, puis cliquez sur **OK**.
7. Sélectionnez les privilèges d'accès de ce rôle.
8. Cliquez sur **Enregistrer tous les rôles**.
9. Cliquez sur **OK**.

Supprimer un rôle personnalisé

Remarque : Si un utilisateur dispose uniquement du rôle supprimé, le système propose de supprimer cet utilisateur en même temps que le rôle.

1. Ouvrez l'espace de travail Configuration.
2. Ouvrez la page Gestion des utilisateurs.
3. Ouvrez l’onglet Rôles.
4. Cliquez sur **Supprimer un rôle**.
   La boîte de dialogue Supprimer un rôle utilisateur s’ouvre.
5. Sélectionnez le rôle à supprimer, puis cliquez sur **OK**.

Exporter et importer les paramètres de gestion des utilisateurs

La base de données de gestion des utilisateurs du logiciel SCIEX OS peut être exportée et importée. Après avoir configuré la base de données de gestion des utilisateurs sur un ordinateur SCIEX, par exemple, exportez-la puis importez-la sur les autres ordinateurs SCIEX afin de vous assurer que les paramètres de gestion des utilisateurs sont cohérents.

Seuls les utilisateurs du domaine sont exportés. Les utilisateurs locaux ne sont pas exportés.

Avant d'importer les paramètres de gestion des utilisateurs, le logiciel sauvegarde automatiquement les réglages actuels. L'utilisateur peut restaurer la dernière sauvegarde.

Exporter les paramètres de gestion des utilisateurs

1. Ouvrez l'espace de travail Configuration.
2. Ouvrez la page Gestion des utilisateurs.
3. Cliquez sur **Avancé** > **Exporter les paramètres de gestion des utilisateurs**.
   La boîte de dialogue Exporter les paramètres de gestion des utilisateurs s'ouvre.
4. Cliquez sur **Parcourir**.
5. Naviguez jusqu'au dossier contenant les paramètres à sauvegarder, sélectionnez-le puis cliquez sur **Sélectionner un dossier**.
6. Cliquez sur **Exporter**.
   Un message de confirmation apparaît, avec le nom du fichier contenant les paramètres exportés.
7. Cliquez sur **OK**.

Importer les paramètres de gestion des utilisateurs

1. Ouvrez l'espace de travail Configuration.
2. Ouvrez la page Gestion des utilisateurs.
3. Cliquez sur **Avancé** > **Importer les paramètres de gestion des utilisateurs**.
   La boîte de dialogue Importer les paramètres de gestion des utilisateurs s'ouvre.
4. Cliquez sur **Parcourir**.
5. Naviguez jusqu'au fichier contenant les paramètres à importer, sélectionnez-le puis cliquez sur **Ouvrir**.
   Le logiciel vérifie la validité du fichier.
6. Cliquez sur **Importer**.
   Le logiciel sauvegarde les paramètres actuels de gestion des utilisateurs et importe les nouveaux paramètres. Un message de confirmation apparaît.
7. Cliquez sur **OK**.

Restaurer les paramètres de gestion des utilisateurs

Avant d'importer les paramètres de gestion des utilisateurs, le logiciel sauvegarde les paramètres actuels. Utilisez cette procédure pour restaurer la dernière sauvegarde des paramètres de gestion des utilisateurs.

1. Ouvrez l'espace de travail Configuration.
2. Ouvrez la page Gestion des utilisateurs.
3. Cliquez sur **Avancé** > **Restaurer les paramètres précédents**.
   La boîte de dialogue Restaurer les paramètres de gestion des utilisateurs s'ouvre.
4. Cliquez sur **Oui**.
5. Fermez le logiciel SCIEX OS, puis rouvrez-le.

Configurer l'accès aux projets et aux fichiers de projet

Utilisez les fonctions de sécurité Windows pour contrôler l'accès au dossier `SCIEX OS Data`. Par défaut, les fichiers de projet sont stockés dans le dossier `SCIEX OS Data`. Pour accéder à un projet, les utilisateurs doivent avoir accès au répertoire racine dans lequel les données du projet sont stockées. Pour plus d'informations, consultez la section Configuration de la sécurité Windows.

Dossiers du projet

Chaque projet contient des dossiers destinés au stockage de différents types de fichiers. Pour obtenir des informations sur le contenu des différents dossiers, consultez le tableau Tableau 4-6.

Tableau 4-6 : Dossiers de projet

Dossier	Contenu
`\Acquisition Methods`	Contient les méthodes spectromètre de masse (MS) et LC créées au sein du projet. Les méthodes MS présentent l'extension msm et les méthodes LC l'extension lcm.
`\Audit Data`	Contient la carte d'audit du projet et tous les enregistrements d'audit.
`\Batch`	Contient tous les fichiers de lot d'acquisition sauvegardés. Les lots d'acquisition ont l'extension bch.
`\Data`	Contient les fichiers de données d'acquisition. Les fichiers de données d'acquisition ont les extensions wiff et wiff2.
`\Project Information`	Contient les fichiers de paramètres par défaut du projet.
`\Quantitation Methods`	Contient tous les fichiers de méthodes de traitement. Les méthodes de traitement ont l'extension .qmethod.

Tableau 4-6 : Dossiers de projet (suite)

Dossier	Contenu
\Quantitation Results	Contient tous les fichiers de quantification du tableau de résultat. Les fichiers du tableau de résultats ont l'extension qsession.

Types de fichier du logiciel

Pour plus d'informations sur les types de fichier courants dans le logiciel SCIEX OS, consultez le Tableau 4-7.

Tableau 4-7 : Fichiers SCIEX OS

Extension	Type de fichier	Dossier
atds	• Données et archives du registre d'audit du poste de travail • Paramètres du registre d'audit du poste de travail • Données du registre d'audit du projet et archives • Paramètres du registre d'audit du projet	• Pour les projets : *<project name>*\Audit Data • Pour le poste de travail : C:\ProgramData\SCIEX\Audit Data
atms	Cartes d'audit	• Pour les projets : *<project name>*\Audit Data • Pour le poste de travail : C:\ProgramData\SCIEX\Audit Data
bch	Lot	Batch
cset	Paramètres du tableau de résultats	Project Information
dad	Fichier de données du spectromètre de masse	• Optimization • Data
exml	Project default settings	Project Information
journal	Fichiers temporaires créés par le logiciel SCIEX OS	Dossiers divers
lcm	Méthode LC	Acquisition Methods
msm	Méthode MS	Acquisition Methods
pdf	Données du document portable	—

Tableau 4-7 : Fichiers SCIEX OS (suite)

Extension	Type de fichier	Dossier
qlayout	Disposition de l'espace de travail	— **Remarque :** La disposition par défaut de l'espace de travail pour un projet est conservée dans le dossier Project Information.
qmethod	Méthode de traitement	Quantitation Methods
qsession	Tableau de résultats du logiciel Tableau de résultats **Remarque :** Le logiciel SCIEX OS ne peut ouvrir que les fichiers qsession créés avec le logiciel SCIEX OS.	Quantitation Results
wiff	Fichier de données de spectrométrie de masse compatible avec le logiciel SCIEX OS **Remarque :** Le logiciel SCIEX OS crée les fichiers wiff et wiff2.	Data
wiff.scan	Fichier de données du spectromètre de masse	• Optimization • Data
wiff2	Fichier de données de spectrométrie de masse généré par le logiciel SCIEX OS	• Optimization • Data
xls ou xlsx	Feuille de calcul Excel	Batch
xps	Réétalonnage	Data\Cal

Central Administrator Console 5

Le logiciel Central Administrator Console (CAC) est une alternative facultative à l'administration locale avec le logiciel SCIEX OS. Le logiciel CAC permet de gérer et personnaliser les rôles, utilisateurs, postes de travail et groupes de travail de manière centralisée.

Cette section décrit le logiciel CAC et explique comment configurer et utiliser cette console pour gérer de façon centralisée les personnes, les projets et les postes de travail.

Remarque : Pour utiliser le logiciel CAC et enregistrer des postes de travail sur le serveur, vérifiez que le logiciel SCIEX OS est installé sur chaque poste de travail.

Le logiciel CAC est activé par une licence et peut être installé sur tout poste de travail compatible avec SCIEX OS version 3.0 et Windows Server 2019.

Le logiciel CAC fait partie du pack d'installation d'SCIEX OS. Toutefois, le logiciel CAC et le logiciel SCIEX OS ne peuvent pas être installés sur le même poste de travail.

Utilisateurs

Utilisez la page Gestion des utilisateurs pour ajouter des utilisateurs et groupes Windows à la base de données de gestion des utilisateurs du logiciel SCIEX OS. L'administrateur peut également ajouter, modifier et supprimer des rôles d'utilisateur dans la section Rôles utilisateur et autorisations. Pour accéder au logiciel, les utilisateurs doivent être définis dans la base de données de gestion des utilisateurs ou être membres d'un groupe défini dans cette base de données.

Groupe d'utilisateurs

Seuls les utilisateurs autorisés peuvent se connecter au poste de travail et accéder au logiciel SCIEX OS lorsque le logiciel SCIEX OS est géré avec le logiciel Central Administrator Console (CAC). Avant de pouvoir ajouter des utilisateurs à des groupes de travail, ils doivent être ajoutés au groupe d'utilisateurs.

Ajouter un utilisateur ou un groupe au groupe d'utilisateurs

1. Ouvrez l'espace de travail Administration centrale.
2. Ouvrez la page Gestion des utilisateurs.
3. Ouvrez l'onglet Groupe d'utilisateurs.
4. Cliquez sur **Ajouter des utilisateurs au groupe d'utilisateurs** ( ). La boîte de dialogue Sélectionner des utilisateurs ou des groupes s'ouvre.
5. Saisissez le nom d'un utilisateur ou d'un groupe, puis cliquez sur **OK**.

Conseil ! Maintenez la touche **Ctrl** enfoncée et cliquez sur **OK** pour sélectionner plusieurs utilisateurs ou groupes.

Supprimer des utilisateurs ou des groupes

1. Ouvrez l'espace de travail Administration centrale.
2. Ouvrez la page Gestion des utilisateurs.
3. Ouvrez l’onglet Groupe d’utilisateurs.
4. Dans le volet de droite, sélectionnez l’utilisateur ou le groupe à supprimer, puis cliquez sur **Supprimer**.
   Le logiciel demande votre confirmation.
5. Cliquez sur **OK**.

Rôles utilisateur et autorisations

Cette section décrit la page Rôles utilisateur et autorisations.

Les utilisateurs peuvent être assignés à un ou plusieurs rôles prédéfinis, décrits dans le tableau suivant, ou à des rôles personnalisés, le cas échéant. Les fonctions auxquelles l’utilisateur a accès sont spécifiées par des rôles. Les rôles prédéfinis ne peuvent pas être supprimés et leurs autorisations ne peuvent pas être modifiées.

Remarque : Dans le logiciel Central Administrator Console (CAC), les utilisateurs peuvent aussi voir la version la plus ancienne de SCIEX OS dans laquelle l’autorisation est prise en charge.

Tableau 5-1 : Rôles prédéfinis

Rôle	Tâches habituelles
Administrateur	• Gère le système • Configure la sécurité
Développeur de méthode	• Crée des méthodes • Exécute des lots • Analyse les données à utiliser par l'utilisateur
Installation d’**Analyst**	• Exécute des lots • Analyse les données à utiliser par l'utilisateur
Examinateur	• Examine les données • Examine les registres d'audit • Examine les résultats de quantification

Tableau 5-2 : Autorisations prédéfinies

Autorisation	Administrateur	Développeur de méthode	Installation d'Analyst	Examinateur
Lot				
Envoyer les méthodes déverrouillées	✓	✓	✓	×
Ouvrir	✓	✓	✓	✓
Enregistrer sous	✓	✓	✓	×
Envoyer	✓	✓	✓	×
Enregistrer	✓	✓	✓	×
Enregistrer le tableau de référence d'ions	✓	✓	✓	×
Ajouter des sous-dossiers de données	✓	✓	✓	×
Configurer les règles de décision	✓	✓	✓	×
Configuration				
Onglet Général	✓	✓	×	×
Général : modifier le paramètre régional	✓	✓	×	×
Général : mode plein écran	✓	✓	×	×
Onglet Communication LIMS	✓	✓	×	×
Général : arrêter les services Windows	✓	×	×	×
Onglet Cartes d'audit	✓	×	×	×
Onglet File d'attente	✓	✓	✓	✓
File d'attente : période d'inactivité de l'instrument	✓	✓	×	×
File d'attente : nombre max. d'échantillons acquis	✓	✓	×	×

Tableau 5-2 : Autorisations prédéfinies (suite)

Autorisation	Administrateur	Développeur de méthode	Installation d'Analyst	Examinateur
File d'attente : autres paramètres de file d'attente	✓	✓	×	×
Onglet Projets	✓	✓	✓	✓
Projets : créer un projet	✓	✓	✓	×
Projets : appliquer un modèle de carte d'audit à un projet	✓	×	×	×
Projets : créer le répertoire racine	✓	×	×	×
Projets : définir le répertoire racine actuel	✓	×	×	×
Projets : spécifier les identifiants réseau	✓	×	×	×
Projets : activer l'écriture de somme de contrôle pour la création de données wiff	✓	×	×	×
Projets : effacer le répertoire racine	✓	×	×	×
Onglet Appareils	✓	✓	✓	×
Onglet Gestion des utilisateurs	✓	×	×	×
Forcer la déconnexion de l'utilisateur	✓	×	×	×
Onglet CAC[1]	✓	×	×	×
Onglet Modèles d'impression	✓	✓	×	×

[1] Dans la version 3.1, l'autorisation **Activer Central Administration** a été renommée en **CAC**. La page CAC dans l'espace de travail Configuration permet de configurer l'administration centrale du logiciel SCIEX OS.

Tableau 5-2 : Autorisations prédéfinies (suite)

Autorisation	Administrateur	Développeur de méthode	Installation d'Analyst	Examinateur
Modèles d'impression : Créer et modifier des modèles d'impression	✓	✓	×	×
Modèles d'impression : Définir le modèle d'impression par défaut	✓	✓	×	×
Modèles d'impression : Appliquer le modèle actuel à tous les projets du répertoire racine	✓	×	×	×
Registre d'événements				
Accéder à l'espace de travail Registre d'événements	✓	✓	✓	✓
Registre d'archive	✓	✓	✓	✓
Trace d'audit				
Accéder à l'espace de travail Trace d'audit	✓	✓	✓	✓
Afficher la carte d'audit active	✓	✓	✓	✓
Imprimer/exporter la trace d'audit	✓	✓	✓	✓
Volet Acquisition des données				
Démarrage	✓	✓	✓	×
Arrêter	✓	✓	✓	×
Enregistrer	✓	✓	✓	×
Méthodes MS et LC				
Accéder à l'espace de travail Méthode	✓	✓	✓	✓
Nouveau	✓	✓	×	×

Tableau 5-2 : Autorisations prédéfinies (suite)

Autorisation	Administrateur	Développeur de méthode	Installation d'Analyst	Examinateur
Ouvrir	✓	✓	✓	✓
Enregistrer	✓	✓	×	×
Enregistrer sous	✓	✓	×	×
Verrouiller/ déverrouiller la méthode	✓	✓	×	×
File d'attente				
Gérer	✓	✓	✓	×
Démarrer/Arrêter	✓	✓	✓	×
Imprimer	✓	✓	✓	✓
Modifier l'échantillon	✓	✓	×	×
Bibliothèque				
Accéder à l'espace de travail Bibliothèque	✓	✓	✓	✓
Réglage MS				
Accéder à l'espace de travail Réglage MS	✓	✓	✓	×
Réglage MS avancé	✓	✓	×	×
Dépannage avancé	✓	✓	×	×
Vérification d'état rapide	✓	✓	✓	×
Restaurer les données de l'instrument	✓	✓	×	×
Analytics				
Nouveaux résultats	✓	✓	✓	×
Créer une méthode de traitement	✓	✓	✓	×
Modifier la méthode de traitement	✓	✓	×	×

Tableau 5-2 : Autorisations prédéfinies (suite)

Autorisation	Administrateur	Développeur de méthode	Installation d'Analyst	Examinateur
Autoriser l'exportation et la création d'un rapport du tableau de résultats déverrouillé	✓	×	×	×
Enregistrer les résultats pour le lot d'automatisation	✓	✓	✓	×
Modifier l'algorithme d'intégration de la méthode de quantification par défaut	✓	✓	×	×
Modifier les paramètres d'intégration de la méthode de quantification par défaut	✓	✓	×	×
Activer l'avertissement de pic modifié du projet	✓	×	×	×
Ajouter des échantillons	✓	✓	✓	×
Supprimer les échantillons sélectionnés	✓	✓	✓	×
Exporter, importer ou supprimer un étalonnage externe	✓	✓	✓	×
Modifier le nom de l'échantillon	✓	✓	✓	×
Modifier le type d'échantillon	✓	✓	✓	×
Modifier l'ID d'échantillon	✓	✓	✓	×
Modifier la concentration réelle	✓	✓	✓	×

Tableau 5-2 : Autorisations prédéfinies (suite)

Autorisation	Administrateur	Développeur de méthode	Installation d'Analyst	Examinateur
Modifier le facteur de dilution	✓	✓	✓	×
Modifier les champs de commentaires	✓	✓	✓	×
Activer l'intégration manuelle	✓	✓	✓	×
Définir le pic comme non trouvé	✓	✓	✓	×
Inclure un pic dans le tableau de résultats ou l'en exclure	✓	✓	✓	×
Options de régression	✓	✓	✓	×
Modifier les paramètres d'intégration du tableau de résultats pour un chromatogramme	✓	✓	✓	×
Modifier la méthode de quantification du composant du tableau de résultats	✓	✓	✓	×
Créer des paramètres de tracé métrique	✓	✓	✓	✓
Ajouter des colonnes personnalisées	✓	✓	✓	×
Définir le format du titre de l'examen des pics	✓	×	×	×
Supprimer la colonne personnalisée	✓	✓	×	×
Paramètres d'affichage du tableau de résultats	✓	✓	✓	✓
Verrouiller le tableau de résultats	✓	✓	✓	✓

Tableau 5-2 : Autorisations prédéfinies (suite)

Autorisation	Administrateur	Développeur de méthode	Installation d'Analyst	Examinateur
Déverrouiller le tableau de résultats	✓	×	×	×
Marquer le fichier de résultats comme révisé et l'enregistrer	✓	×	×	✓
Modifier le modèle de rapport	✓	✓	×	×
Transférer les résultats à LIMS	✓	✓	✓	×
Modifier la colonne de code-barres	✓	✓	×	×
Modifier l'affectation d'échantillon de comparaison	✓	✓	×	×
Ajouter les spectres MSMS à la bibliothèque	✓	✓	×	×
Paramètres par défaut du projet	✓	✓	×	×
Créer un rapport dans tous les formats	✓	✓	✓	✓
Modifier les paramètres du critère de marquage	✓	✓	✓	×
Modification du paramètre de suppression automatique des données aberrantes	✓	✓	×	×
Activer la suppression automatique des données aberrantes	✓	✓	✓	×
Mettre à jour la méthode de traitement via FF/LS	✓	✓	×	×

Tableau 5-2 : Autorisations prédéfinies (suite)

Autorisation	Administrateur	Développeur de méthode	Installation d'Analyst	Examinateur
Mettre à jour les résultats via FF/LS	✓	✓	×	×
Activer la fonction de regroupement par adduits	✓	✓	×	×
Rechercher des fichiers	✓	✓	✓	✓
Activer l'ajout de standards	✓	✓	✓	×
Définir la règle de pourcentage d'intégration manuelle	✓	×	×	×
Modifier le poids/ volume	✓	✓	✓	×
Explorateur				
Accéder à l'espace de travail Explorateur	✓	✓	✓	✓
Exporter	✓	✓	✓	×
Imprimer	✓	✓	✓	×
Options	✓	✓	✓	×
Réétalonner	✓	✓	×	×

Ajouter un rôle personnalisé

Le logiciel Central Administrator Console (CAC) contient quatre rôles prédéfinis. Si des rôles supplémentaires sont nécessaires, copiez un rôle existant et affectez des droits d'accès.

1. Ouvrez l'espace de travail Administration centrale.
2. Ouvrez la page Gestion des utilisateurs.
3. Ouvrez l'onglet Rôles utilisateur et autorisations.
4. Cliquez sur **Ajouter un rôle** ( ).
   La boîte de dialogue Dupliquer un rôle utilisateur s'ouvre.

5. Dans le champ **Rôle utilisateur existant**, sélectionnez le rôle à utiliser comme modèle pour le nouveau rôle.
6. Entrez un nom et une description pour le rôle, puis cliquez sur **OK**.
   Le nouveau rôle s'affiche dans la fenêtre Rôles utilisateur et catégories d'autorisations.
7. Sélectionnez les privilèges d’accès pour le rôle en cochant les cases appropriées.
8. Cliquez sur **Enregistrer tous les rôles**.

Supprimer un rôle personnalisé

1. Ouvrez l'espace de travail Administration centrale.
2. Ouvrez la page Gestion des utilisateurs.
3. Ouvrez l’onglet Rôles utilisateur et autorisations.
4. Cliquez sur **Supprimer un rôle**.
   La boîte de dialogue Supprimer un rôle utilisateur s’ouvre.
5. Sélectionnez le rôle à supprimer, puis cliquez sur **OK**.

Groupes de travail

Utilisez la page Gestion des groupes de travail pour gérer des groupes de travail. Les groupes de travail comportent des utilisateurs, des postes de travail et des projets.

Créez un groupe de travail en ajoutant des ressources de leurs groupes respectifs. Avant de créer des groupes de travail, veillez à ajouter tous les utilisateurs potentiels au groupe d’utilisateurs, les postes de travail au groupe de postes de travail et les répertoires racine du projet au groupe de projets.

Ajoutez des rôles supplémentaires si nécessaire. Éventuellement, sélectionnez le mode de sécurité de chaque groupe de travail.

Le mode de sécurité paramétré pour le groupe de travail est prioritaire sur le mode de sécurité paramétré pour le poste de travail, si ce dernier est enregistré avec le logiciel Central Administrator Console (CAC) et fait partie du groupe de travail.

N’ajoutez pas d’utilisateurs locaux aux groupes de travail. Le logiciel CAC est une application réseau, et seuls les utilisateurs du réseau doivent être ajoutés à un groupe de travail.

Remarque : Dans chaque groupe de travail, au moins utilisateur doit recevoir le rôle d'administrateur. Seul un administrateur ou un superviseur peut déverrouiller l’écran du logiciel CAC si l’utilisateur actuellement connecté est indisponible.

Si la sécurité sur serveur n’est plus requise pour un poste de travail particulier, gérez la sécurité de ce poste en local avec le logiciel SCIEX OS.

Créer un groupe de travail

1. Ouvrez l'espace de travail Administration centrale.
2. Ouvrez la page Gestion des groupes de travail.

3. Cliquez sur **Ajouter un groupe de travail** ().
   La boîte de dialogue Ajouter un groupe de travail s'ouvre.
4. Saisissez un nom dans le champ **Nom du groupe de travail**.
5. Saisissez une description dans le champ **Description**, puis cliquez sur **Ajouter**.
   Le groupe de travail est créé et ajouté au volet Gérer les groupes de travail et les associations. Le logiciel Central Administrator Console (CAC) crée le nom de groupe de travail approprié sur le serveur.

   Remarque : Le mode intégré est le paramètre de sécurité par défaut.

Supprimer un groupe de travail

Si un groupe de travail n'est plus nécessaire, supprimez-le de la liste des groupes de travail. La suppression d'un groupe de travail fait seulement disparaître le groupe de travail du logiciel Central Administrator Console (CAC). Aucune donnée du poste de travail n'est perdue.

1. Ouvrez l'espace de travail Administration centrale.
2. Ouvrez la page Gestion des groupes de travail.
3. Développez la liste **Groupes de travail** et repérez le groupe de travail à supprimer. Cliquez sur **Supprimer**.
   La boîte de dialogue Supprimer un groupe de travail s'ouvre.
4. Cliquez sur **Oui**.

Ajouter des utilisateurs ou des groupes à un groupe de travail

Remarque : Les utilisateurs ajoutés au groupe de travail n'ont pas de rôle affecté automatiquement. Pour affecter des rôles aux utilisateurs, consultez la section Ajouter ou supprimer un rôle.

1. Ouvrez l'espace de travail Administration centrale.
2. Ouvrez la page Gestion des groupes de travail.
3. Dans le volet Gérer les groupes de travail et les associations, développez le groupe de travail à modifier, puis développez la liste **Utilisateurs**.
4. Sélectionnez un utilisateur ou un groupe et cliquez sur **Ajouter** ().

   Conseil ! Ajoutez ou sélectionnez des utilisateurs multiples en appuyant sur **Maj** puis en sélectionnant les utilisateurs souhaités.

   L'utilisateur ou le groupe est ajouté au groupe de travail actuel.
5. Affectez un ou plusieurs rôles à l'utilisateur ou au groupe ajouté. Consultez la section Ajouter ou supprimer un rôle.

6. Cliquez sur **Enregistrer**.

Ajouter ou supprimer un rôle

Procédures préalables
• Ajouter des utilisateurs ou des groupes à un groupe de travail.

Pour plus d'informations sur la création de rôles dans le logiciel Central Administrator Console (CAC), consultez la section Ajouter un rôle personnalisé. Les utilisateurs ou les groupes avec un rôle affecté ont toutes les autorisations associées à ce rôle. Les utilisateurs ou les groupes peuvent avoir plusieurs rôles à la fois.

1. Ouvrez l'espace de travail Administration centrale.
2. Ouvrez la page Gestion des groupes de travail.
3. Dans le volet Gérer les groupes de travail et les associations, développez le groupe de travail à modifier, puis développez la liste **Utilisateurs**.
4. Dans la section Appartenance au groupe de travail actuel, attribuez ou retirez des rôles dans la colonne **Attribuer les rôles**.
5. Cliquez sur **Enregistrer**.

Ajouter des postes de travail à un groupe de travail

Remarque : Un poste de travail ne s'affiche dans le groupe de postes de travail que s'il a été enregistré avec le logiciel Central Administrator Console (CAC). Consultez la section Ajouter un poste de travail.

1. Ouvrez l'espace de travail Administration centrale.
2. Ouvrez la page Gestion des groupes de travail.
3. Dans le volet Gérer les groupes de travail et les associations, développez le groupe de travail à modifier, puis développez la liste **Postes de travail**.
4. Sélectionnez un poste de travail et cliquez sur **Ajouter** ().
   Le poste de travail est ajouté au groupe de travail actuel.
5. Cliquez sur **Enregistrer**.

Attribuer des paramètres de sécurité de groupe de travail

Procédures préalables
• Ajouter un poste de travail • Ajouter des postes de travail à un groupe de travail

Pour plus d'informations sur les modes de sécurité, consultez la section Configurer le mode de sécurité.

1. Ouvrez l'espace de travail Administration centrale.
2. Ouvrez la page Gestion des groupes de travail.
3. Dans le volet Gérer les groupes de travail et les associations, développez le groupe de travail à modifier, puis développez la liste **Postes de travail**.
4. (Facultatif) Pour définir le groupe de travail actuel comme groupe de travail par défaut pour ce poste de travail, cochez la case **Définir la valeur par défaut** dans la section Appartenance au groupe de travail actuel.
5. Dans la section Attribuer les paramètres de sécurité, sélectionnez le mode de sécurité du groupe de travail dans le champ **Mode de sécurité**, puis saisissez les durées appropriées dans les champs **Verrouillage de l'écran** et **Déconnexion automatique**.
6. Cliquez sur **Enregistrer**.

Ajouter des projets à un groupe de travail

Remarque : Cette procédure n'est nécessaire que si l'accès au projet est géré de manière centralisée.

Remarque : Si un projet est ajouté à plusieurs groupes de travail, l'accès de l'utilisateur à ce projet est ajouté et non écrasé. Par exemple, le Workgroup 1 contient User A, User B et Project_01. Le Workgroup 2 contient User B et User C. Si le Project_01 est ajouté à Workgroup 2, alors User A, User B, et User C auront tous accès à Project_01.

1. Ouvrez l'espace de travail Administration centrale.
2. Ouvrez la page Gestion des groupes de travail.
3. Dans le volet Gérer les groupes de travail et les associations, développez le groupe de travail à modifier, puis développez la liste **Projets**.
4. Cochez la case **Utiliser les paramètres centraux pour les projets**.
   La section de sélection des projets est affichée.
5. Sélectionnez un **Répertoire de racine de projet** pour ajouter un groupe entier de projets ou développez la racine du projet et sélectionnez un projet spécifique à ajouter au groupe de travail.
6. Cliquez sur **Ajouter** () pour ajouter les projets au groupe de travail.
   La racine du projet est ajoutée au tableau Appartenance au groupe de travail actuel. Développez la racine de projet pour afficher les projets actuels dans le groupe de travail.
7. Cliquez sur **Enregistrer**.

Gérer des projets

Utilisez la page Gestion de projet pour créer, modifier et supprimer des projets.

Pour accéder à un projet, les utilisateurs doivent avoir accès au répertoire racine dans lequel les données du projet sont stockées. Pour plus d'informations, consultez la section À propos des projets et des répertoires racines.

À propos des projets et des répertoires racines

Un répertoire racine est un dossier contenant un ou plusieurs projets. C'est le dossier dans lequel le logiciel recherche des données du projet. Le répertoire racine prédéfini est `D:\SCIEX OS Data`.

Pour vous assurer que les informations relatives au projet sont stockées en toute sécurité, créez des projets avec le logiciel Central Administrator Console (CAC). Ajoutez des projets au Répertoire racine de projet avant de les ajouter à un groupe de travail. Consultez la section Ajouter un projet.

Les données de projet peuvent être organisées en sous-dossiers. Créez les sous-dossiers avec le logiciel CAC. Consultez la section Ajouter un sous-dossier.

Remarque : Si un projet est créé en dehors du logiciel CAC, la racine du projet doit être actualisée après la création du projet. Une fois la racine actualisée, le contenu du Répertoire racine de projet est synchronisé avec le contenu des racines de projet sur le réseau.

Ajouter un répertoire racine

Le répertoire racine est le dossier dans lequel un ou plusieurs projets sont stockés.

Remarque : Le logiciel sauvegarde jusqu'à dix répertoires racines.

Conseil ! Les disques locaux ne sont pas accessibles sur le réseau. Un répertoire racine ne peut être créé que sur un disque partagé.

1. Ouvrez l'espace de travail Administration centrale.
2. Ouvrez la page Gestion de projet.
3. Cliquez sur **Ajouter une racine de projet (nouvelle ou existante) au groupe de projets** ( ).
   La boîte de dialogue Ajouter un répertoire racine s'ouvre.
4. Saisissez le chemin d'accès complet au répertoire racine puis cliquez sur **OK**.
   Le dossier est créé.

   Conseil ! Au lieu de saisir le chemin, cliquez sur **Parcourir**, puis sélectionnez le dossier dans lequel le répertoire racine sera créé.

   Conseil ! Vous pouvez aussi créer un dossier dans l'explorateur de fichiers, puis naviguer jusqu'à ce dossier et le sélectionner.

Remarque : Lorsque le logiciel SCIEX OS est installé avec une licence de traitement, le répertoire racine peut être un dossier du logiciel Analyst (`Analyst Data\Projects`).

5. Cliquez sur **OK**.
   Le nouveau répertoire racine devient le répertoire racine du projet actuel.

Supprimer un répertoire racine de projet

Le logiciel maintient une liste d'au moins les dix derniers répertoires racines utilisés. L'utilisateur peut supprimer des répertoires racines de cette liste.

Remarque : La suppression d'un répertoire racine de projet entraîne également la suppression de tous les projets associés depuis le groupe racine de projet.

1. Ouvrez l'espace de travail Administration centrale.
2. Ouvrez la page Gestion de projet.
3. Trouvez le répertoire racine de projet à supprimer et cliquez sur **Supprimer une racine de projet** dans la section Actions.
   Le logiciel demande votre confirmation.
4. Cliquez sur **OK**.

Ajouter un projet

Procédures préalables
• Ajouter un répertoire racine

Le projet conserve les méthodes d'acquisition, les données, les lots, les méthodes de traitement, les résultats de traitement, etc. Nous recommandons d'utiliser un dossier de projet distinct pour chaque projet.

Ne créez pas de projets et ne copiez pas ou ne collez pas de fichiers en dehors du logiciel Central Administrator Console (CAC).

1. Ouvrez l'espace de travail Administration centrale.
2. Ouvrez la page Gestion de projet.
3. Cliquez sur **Ajouter un projet** dans la section Actions du dossier racine.
   La boîte de dialogue Nouveau projet s'ouvre.
4. Saisissez le nom du projet.
5. Cliquez sur **OK**.
   Le nouveau projet est affiché sous la racine du projet.

Ajouter un sous-dossier

Les données dans les projets peuvent être organisées en sous-dossiers.

1. Ouvrez l'espace de travail Administration centrale.
2. Ouvrez la page Gestion de projet.
3. Cliquez sur **Ajouter des sous-dossiers de données** dans la section Actions du dossier racine.
   La boîte de dialogue Ajouter des sous-dossiers de données s'ouvre.
4. Sélectionnez un projet auquel appartiendra le sous-dossier.
5. Cliquez sur **Ajouter un nouveau sous-dossier de données** ().
   La boîte de dialogue Nom du sous-dossier de données s'ouvre.
6. Saisissez le nom du sous-dossier.
7. Cliquez sur **Enregistrer**.

Conseil ! Les sous-dossiers peuvent être imbriqués dans d'autres sous-dossiers. Pour créer un sous-dossier imbriqué, sélectionnez un sous-dossier dans la section Sous-dossiers de données de projet puis cliquez sur **Ajouter un nouveau sous-dossier de données** ().

8. Fermez la boîte de dialogue Ajouter des sous-dossiers de données.

Postes de travail

Utilisez la page Gestion des postes de travail pour gérer tous les postes de travail connectés au logiciel CAC. Les paramètres personnalisés sont automatiquement appliqués aux postes de travail sous le contrôle du logiciel CAC.

Ajouter un poste de travail

Sur la page Gestion des postes de travail, les administrateurs peuvent ajouter des postes de travail, activer ou désactiver le contrôle central des postes de travail, et supprimer des postes de travail.

1. Ouvrez l'espace de travail Administration centrale.
2. Ouvrez la page Gestion des postes de travail.
3. Cliquez sur **Ajouter un poste de travail au groupe de postes de travail** ().
   La boîte de dialogue Sélectionner des ordinateurs s'ouvre.
4. Saisissez les noms des postes de travail à ajouter et cliquez sur **OK**.
   Le champ **État** d'administration centrale du poste de travail passe de **Connexion en cours** à **Désactivé**.
5. (Facultatif) Pour activer le contrôle central du poste de travail, procédez comme suit :
   a. Dans la colonne **État**, cliquez sur **Désactivé**.

b. Cliquez sur **OK**.

Conseil ! Les utilisateurs peuvent également activer l'administration centrale dans le logiciel SCIEX OS. Consultez le *Système d'aide du logiciel SCIEX OS*.

Supprimer un poste de travail

Si un poste de travail n'est plus utilisé ou n'est plus nécessaire dans un groupe de travail, supprimez-le de ce dernier. Si un poste de travail est supprimé, il est retiré de tous les groupes de travail auxquels il était associé. Aucune donnée n'est perdue sur le poste de travail lors de sa suppression.

1. Ouvrez l'espace de travail Administration centrale.
2. Ouvrez la page Gestion des postes de travail.
3. Cliquez sur **Gestion des postes de travail**.
4. Dans le volet Groupe de postes de travail, trouvez le poste de travail à supprimer, puis cliquez sur **Supprimer**.
   La boîte de dialogue Supprimer un poste de travail s'ouvre.
5. Cliquez sur **OK**.

Rapports et fonctions de sécurité

Générer des rapports de données

Utilisez cette procédure pour générer des rapports de données comprenant des informations telles que les utilisateurs, rôles, postes de travail, projets et groupes de travail configurés.

1. Ouvrez l'espace de travail Administration centrale.
2. Cliquez sur **Imprimer**.
   La boîte de dialogue Options d'impression s'ouvre.
3. Sélectionner les pages à imprimer et cliquez sur **Continuer**.
4. Configurez les options d'impression, puis cliquez sur **Imprimer**.
5. (Imprimer en PDF uniquement) Naviguez jusqu'à l'emplacement d'enregistrement du rapport et cliquez sur **Enregistrer**.

Exporter les paramètres de CAC du logiciel

Utilisez cette procédure pour exporter les paramètres de sécurité et pouvoir les importer dans un autre système Central Administrator Console (CAC). Les paramètres sont exportés dans un fichier `ecac`.

1. Ouvrez l'espace de travail Administration centrale.
2. Cliquez sur **Avancé** > **Exporter les paramètres CAC**.
   La boîte de dialogue Exporter les paramètres CAC s'ouvre.
3. Cliquez sur **Parcourir**.

4. Naviguez jusqu'au dossier contenant les paramètres à sauvegarder, sélectionnez-le puis cliquez sur **Sélectionner un dossier**.
5. Cliquez sur **Exporter**.
   Un message de confirmation apparaît, avec le nom du fichier contenant les paramètres exportés.
6. Cliquez sur **OK**.

Importer les paramètres logiciels de CAC

Procédures préalables
• Exporter les paramètres de CAC du logiciel

Utilisez cette procédure pour importer les paramètres de sécurité d'autres systèmes Central Administrator Console (CAC). Les paramètres sont importés depuis un fichier `ecac`.

1. Ouvrez l'espace de travail Administration centrale.
2. Ouvrez l'espace de travail Configuration.
3. Ouvrez la page Gestion des utilisateurs.
4. Cliquez sur **Avancé** > **Importer les paramètres CAC**.
   La boîte de dialogue Importer les paramètres CAC s'ouvre.
5. Cliquez sur **Parcourir**.
6. Naviguez jusqu'au fichier contenant les paramètres à importer, sélectionnez-le puis cliquez sur **Ouvrir**.
   Le logiciel vérifie la validité du fichier.
7. Cliquez sur **Importer**.
   Le logiciel sauvegarde les paramètres actuels puis importe les nouveaux paramètres.
   Un message de confirmation apparaît.

   Remarque : Les paramètres importés sont appliqués après le redémarrage du logiciel .
8. Cliquez sur **OK**.

Restaurer les paramètres du logiciel CAC

Utilisez cette procédure pour importer automatiquement les derniers paramètres `ecac` exportés.

1. Ouvrez l'espace de travail Administration centrale.
2. Cliquez sur **Avancé** > **Restaurer les paramètres CAC**.
   La boîte de dialogue Restaurer les paramètres CAC s'ouvre.

   Remarque : Les paramètres restaurés sont appliqués après le redémarrage du logiciel Central Administrator Console (CAC).

3. Cliquez sur **Oui**.

Exporter les paramètres de gestion des utilisateurs de CAC

Utilisez cette procédure pour exporter les paramètres de gestion des utilisateurs, pouvant être appliqués à un autre système Central Administrator Console (CAC). Les paramètres sont exportés dans un fichier `data`.

Remarque : Les paramètres exportés ne peuvent être importés que dans un système utilisant la même version du logiciel CAC.

1. Ouvrez l'espace de travail Gestion de la configuration.
2. Cliquez sur **Avancé** > **Exporter les paramètres de gestion des utilisateurs**.
   La boîte de dialogue Exporter les paramètres CAC s'ouvre.
3. Cliquez sur **Parcourir**.
4. Naviguez jusqu'au dossier contenant les paramètres à sauvegarder, sélectionnez-le puis cliquez sur **Sélectionner un dossier**.
5. Cliquez sur **Exporter**.
   Un message de confirmation apparaît, avec le nom du fichier contenant les paramètres exportés.
6. Cliquez sur **OK**.

Importer les paramètres de gestion des utilisateurs CAC

Procédures préalables
• Exporter les paramètres de gestion des utilisateurs de CAC

Utilisez cette procédure pour importer les paramètres de sécurité d'un autre système Central Administrator Console (CAC). Les paramètres sont importés depuis un fichier `data`.

Remarque : Les paramètres exportés ne peuvent être importés que dans un système utilisant la même version du logiciel CAC.

1. Ouvrez l'espace de travail Gestion de la configuration.
2. Cliquez sur **Avancé** > **Importer les paramètres de gestion des utilisateurs**.
   La boîte de dialogue Importer les paramètres de gestion des utilisateurs s'ouvre.
3. Cliquez sur **Parcourir**.
4. Naviguez jusqu'au fichier contenant les paramètres à importer, sélectionnez-le puis cliquez sur **Ouvrir**.
   Le logiciel vérifie la validité du fichier.
5. Cliquez sur **Importer**.
   Le logiciel sauvegarde les paramètres actuels puis importe les nouveaux paramètres.
   Un message de confirmation apparaît.

Remarque : Les paramètres importés sont appliqués après le redémarrage du logiciel CAC.

6. Cliquez sur **OK**.

Acquisition réseau 6

Cette section décrit le fonctionnement de l'acquisition réseau dans le logiciel SCIEX OS ainsi que les avantages et limites des projets en réseau. Elle contient également les procédures de configuration de l'acquisition réseau.

À propos de l'acquisition réseau

L'acquisition réseau peut être utilisée pour l'acquisition de données depuis un ou plusieurs instruments vers des dossiers de projet sur le réseau pouvant être traités sur des postes de travail distants. Ce processus est tolérant aux pannes de réseau et garantit qu'aucune donnée ne sera perdue en cas de panne de la connexion réseau durant l'acquisition.

Les performances du système peuvent être plus lentes lors de l'utilisation de projets en réseau qu'avec des projets locaux. Certains registres d'audit résidant également dans les dossiers en réseau, toute activité qui génère un enregistrement d'audit de projet est également ralentie. Les fichiers en réseau peuvent mettre un certain temps à s'ouvrir, selon les performances du réseau. Les performances du réseau sont liées non seulement au matériel physique du réseau, mais également à son trafic et à sa conception.

Remarque : Si le service ClearCore2 est interrompu au cours d'une acquisition réseau, les données partielles de l'échantillon en cours d'acquisition au moment de l'interruption ne sont pas écrites dans le fichier de données.

Remarque : Lorsque vous utilisez l'acquisition réseau dans un environnement réglementé, synchronisez l'heure locale de l'ordinateur avec l'heure du serveur pour que les estampilles temporelles soient exactes. L'heure du serveur est utilisée comme heure de création du fichier. L'Audit Trail Manager enregistre l'heure de création du fichier à l'aide de l'heure de l'ordinateur local.

ATTENTION : Risque de perte de données. N'enregistrez pas de données provenant de plusieurs ordinateurs d'acquisition vers le même fichier de données en réseau.

Avantages de l'utilisation de l'acquisition réseau

L'acquisition de données en réseau fournit une méthode de travail sécurisée avec des dossiers de projet intégralement placés sur les serveurs réseau. Cela réduit la complexité inhérente au recueil de données localement puis le transfert des données vers un emplacement réseau pour le stockage. De même, puisque les lecteurs réseau sont en principe automatiquement sauvegardés, la nécessité de sauvegarder les lecteurs locaux est moindre ou inutile.

Compte réseau sécurisé

Dans un environnement régulé où les données sont acquises dans un dossier réseau, il est vivement recommandé que les utilisateurs ne disposent pas de droits de suppression pour le dossier de destination. Cependant, sans accès en suppression à ce dossier, le logiciel SCIEX OS ne peut pas fonctionner correctement. La fonctionnalité de compte réseau sécurisé (SNA) identifie un compte réseau avec autorisation de contrôle complet sur les fichiers pour le répertoire racine du réseau. Le service ClearCore2 utilise ce compte pour transférer des données vers le dossier réseau.

Le SNA doit avoir le contrôle complet sur :

- Le dossier du répertoire racine du réseau
- Le dossier `SCIEX OS Data\NetworkBackup` sur l'ordinateur d'acquisition
- Le dossier `SCIEX OS Data\TempData` sur l'ordinateur d'acquisition

Le SNA n'a pas besoin de :

- Appartenir au groupe Administrator sur l'ordinateur.
- Figurer dans la base de données de gestion des utilisateurs du logiciel SCIEX OS.

Le compte SNA est spécifié sur la page Projets de l'espace de travail Configuration. Il n'est possible de spécifier qu'un compte de domaine ou réseau Windows valide.

Si aucun compte SNA n'est spécifié, le logiciel SCIEX OS utilise les identifiants de l'utilisateur connecté pour transférer les données vers le répertoire racine du réseau. Pour que le transfert aboutisse, le compte doit disposer d'autorisations d'écriture sur tous les dossiers de projet dans lesquels des données sont récupérées, quel que soit l'utilisateur qui a soumis le lot pour acquisition.

Processus de transfert de données

Lorsque SCIEX OS procède à l'acquisition de données à un emplacement réseau, il consigne chaque échantillon dans un dossier local, puis transfère les données vers l'emplacement réseau. Lorsque le transfert du fichier complet de données est confirmé, le dossier local contenant les données est supprimé. Si le réseau est inaccessible au cours du processus, SCIEX OS réessaie toutes les 15 minutes jusqu'à ce que le transfert aboutisse.

Pour plus d'informations sur l'accès aux données pendant des pertes prolongées de connectivité réseau, consultez la section Retirer des échantillons des dossiers de transfert réseau.

Configurer l'acquisition réseau

Un répertoire racine est le dossier dans lequel le logiciel SCIEX OS stocke les données. Pour être sûr que les informations du projet sont stockées en toute sécurité, créez le répertoire racine à l'aide du logiciel SCIEX OS. Ne créez pas de projets dans l'Explorateur de fichiers.

Éventuellement, lorsque vous créez des répertoires racines sur une ressource réseau, définissez les identifiants **Identifiants du compte réseau sécurisé**. Il s'agit du compte réseau sécurisé défini sur la ressource en réseau. Consultez la section Compte réseau sécurisé.

Pour plus d'informations sur la création de projets et de sous-projets, consultez le document *Guide de l'utilisateur du logiciel SCIEX OS*.

Spécifier un compte réseau sécurisé

Si des projets sont stockés sur une ressource réseau, un compte réseau sécurisé (SNA) peut être spécifié pour s'assurer que tous les utilisateurs du poste de travail disposent des droits d'accès requis pour cette ressource.

1. Ouvrez l'espace de travail Configuration.
2. Cliquez sur **Projets**.
3. Dans la section **Avancé**, cliquez sur **Identifiants du compte réseau sécurisé**.
4. Saisissez le nom d'utilisateur, le mot de passe et le domaine du compte réseau sécurisé défini sur la ressource réseau.
5. Cliquez sur **OK**.

Audit 7

Cette section explique comment utiliser la fonctionnalité d'audit. Pour obtenir des informations sur les fonctions d'audit de Windows, consultez la section Audits du système.

Registres d’audit

Le logiciel organise les événements d'audit dans l’espace de travail Trace d'audit. Le logiciel stocke les événements dans les registres d'audit, qui sont des fichiers contenant les enregistrements des événements audités.

Les événements du poste de travail sont stockés dans le registre d'audit du poste de travail. Les registres d'audit de poste de travail sont des fichiers qui conservent les événements audités pour l’ordinateur sur lequel le logiciel SCIEX OS est installé.

Les événements du système CAC sont stockés dans le registre d'audit de CAC.

Les événements du projet sont stockés dans le registre d'audit du projet. L’espace de travail Trace d'audit affiche les registres d'audit des projets dans le répertoire racine actif. Les événements du registre d'audit de traitement sont contenus dans le registre d'audit du projet. Ils sont stockés avec le tableau de résultats.

Pour obtenir la liste complète des événements audités, consultez la section Événements d'audit.

Les registres d'audit, associés à des fichiers `wiff2` et des tableaux de résultats, sont des enregistrements électroniques valides pouvant être utilisés à des fins de conformité.

Tableau 7-1 : Registres d'audit

Registre d'audit	Exemples d'événements enregistrés	Cartes d'audit disponibles enregistrées dans	Cartes d'audit par défaut

Poste de travail (SCIEX OS)	• Modifications apportées :
	  • Attribution de la carte d'audit active
	  • Réglage de l'instrument
	  • Files d'attente d'échantillons
	  • Sécurité
	  • Ajustement
	  • Appareils
		• Dossier `C:\ProgramData\SCIEX\Audit Data`	• Pas de carte d'audit

CAC	• Modifications apportées :
	  • Carte d'audit
	  • CAC
	  • Sécurité
	  • Registre d'utilisateurs
		• Dossier `C:\ProgramData\SCIEX\Audit Data`	• Carte d'audit silencieuse

Projet (un par projet)	• Modifications apportées :
	  • Attribution de la carte d'audit active (SCIEX OS)
	  • Projet
	  • Données
	• Impression
		• Dossier *<project>*`\Audit Data`	• Spécifié sur la page Cartes d'audit de l'espace de travail Configuration

Lorsqu'un registre d'audit contient 20 000 enregistrements, les logiciels SCIEX OS et CAC archivent automatiquement les enregistrements et démarrent un nouveau registre d'audit. Pour plus d'informations, consultez la section Archives de registres d'audit.

Cartes d'audit

Une carte d’audit est un fichier contenant une liste de tous les événements pouvant être audités et indiquant si une raison d’apporter une modification ou une signature électronique est requise pour l’événement. Dans le logiciel SCIEX OS, deux types de carte d'audit sont disponibles : poste de travail et projet. Dans le logiciel CAC, deux types de carte d'audit sont disponibles : CAC et projet.

Les cartes d'audit de poste de travail contrôlent les événements qui sont audités sur un poste de travail.

Les cartes d'audit de projet contrôlent les événements qui sont audités pour un projet et conservés dans le dossier de projet.

Remarque : La carte d'audit d’un projet peut être modifiée dans le logiciel SCIEX OS ou Central Administrator Console (CAC).

L'utilisateur peut créer plusieurs cartes d'audit, mais une seule carte d'audit peut être utilisée à la fois pour chaque poste de travail, système CAC et chaque projet. La carte d'audit utilisée pour un poste de travail, un système CAC ou un projet est appelée carte d'audit active.

Lorsque le logiciel SCIEX OS est installé, la carte d'audit par défaut de tous les nouveaux projets est No Audit Map. Lorsque le logiciel CAC est installé, la carte d'audit par défaut pour tous les nouveaux projets est Silent Audit Map. L’utilisateur peut identifier une autre carte d'audit active à utiliser par défaut pour tous les nouveaux projets. Consultez la section Modifier la carte d'audit active d'un projet.

Configuration des cartes d'audit

Avant de travailler sur des projets nécessitant un audit, configurez des cartes d'audit applicables aux procédures de fonctionnement standard. Plusieurs modèles de carte d'audit par défaut sont disponibles lors de l'installation du logiciel, mais il peut s'avérer nécessaire de créer une carte personnalisée. Assurez-vous d'avoir une carte d’audit pour le registre d'audit du poste de travail ou de CAC, et une carte d’audit pour chaque projet.

Tableau 7-2 : Liste de contrôle pour la configuration de l’audit

Tâche	Consulter

• SCIEX OS : Créer une carte d'audit pour le registre d'audit du poste de travail.
• Logiciel CAC : Créer une carte d'audit pour le registre d'audit de CAC.
	• SCIEX OS :
	  • Créer une carte d'audit de poste de travail
	  • Modifier une carte d'audit de poste de travail
	• Logiciel CAC :
	  • Créer une carte d’audit CAC
	  • Modifier une carte d’audit CAC

Tableau 7-2 : Liste de contrôle pour la configuration de l’audit (suite)

Tâche	Consulter
• SCIEX OS : Appliquer la carte d'audit au registre d'audit du poste de travail. • Logiciel CAC : Appliquer la carte d'audit au registre d'audit de CAC.	• SCIEX OS: Modifier la carte d'audit active d'un poste de travail • Logiciel CAC : Modifier la carte d'audit active d’un système CAC
Créer une carte d'audit active par défaut pour de nouveaux projets.	• Créer une carte d'audit de projet.
Configurer la carte d'audit à utiliser pour chaque projet existant.	• Créer une carte d'audit de projet. • Modifier une carte d'audit de projet.
Appliquer une carte d'audit à chaque projet existant.	• Modifier la carte d'audit active d'un projet.

Modèles de carte d'audit installés

Le logiciel comprend plusieurs modèles de carte d’audit. Ces modèles ne peuvent être ni modifiés ni supprimés.

Tableau 7-3 : Cartes d'audit installées

Carte d'audit	Description
Exemple de carte d'audit	Les événements sélectionnés sont audités. À des fins d'illustration uniquement.
Carte d'audit complète	Tous les événements sont audités. Des signatures électroniques et des motifs sont nécessaires pour l'ensemble des événements.
Aucune carte d'audit	Aucun événement n'est audité. **Remarque :** L'événement **Modifier l'affectation de carte d'audit active** est toujours enregistré, même si le modèle Pas de carte d'audit est utilisé.
Carte d'audit silencieuse	Tous les événements sont audités. Les événements ne nécessitent aucune signature électronique et aucun motif.

Pour obtenir une description des différents types de registre d'audit et leurs liens avec les cartes d'audit, consultez le Tableau 7-1. Pour plus d'informations sur les événements enregistrés dans les registres d'audit, consultez la section Enregistrements de registre d'audit SCIEX OS.

Pour obtenir des informations sur le processus d’audit, consultez le Tableau 7-2.

Travailler avec des cartes d'audit

Le logiciel comprend plusieurs modèles de carte d'audit installés. Pour obtenir des descriptions des modèles de carte d'audit, consultez la section Modèles de carte d'audit installés. Pour obtenir une liste de vérification des étapes suggérées pour la configuration de l'audit, consultez la section Configuration des cartes d'audit.

Si un modèle de carte d'audit actif est supprimé dans le logiciel ou dans File Explorer, le projet qui l'emploie utilise la carte d'audit silencieuse.

Cartes d'audit de projet

Les cartes d'audit de projet contrôlent l'audit des événements du projet. Pour obtenir la liste des événements du projet pouvant être audités, consultez la section Registre d'audit du projet.

Créer une carte d'audit de projet

1. Ouvrez l'espace de travail Configuration.
2. Cliquez sur **Cartes d'audit**.
3. Ouvrez l'onglet Modèles de projet.
4. Dans le champ **Modifier le modèle de carte**, sélectionnez un modèle à utiliser comme base de la nouvelle carte.
5. Cliquez sur **Ajouter un modèle** ().
   La boîte de dialogue Ajouter un modèle de carte d'audit de projet s'ouvre.
6. Cliquez sur le nom de la nouvelle carte, puis sur **OK**.
7. Sélectionnez et configurez les événements à enregistrer en respectant la procédure suivante :
   a. Cochez la case **Audité** pour l'événement.
   b. (Facultatif) Si une raison est requise, sélectionnez **Motif requis**.
   c. (Facultatif) Si une signature électronique est requise, sélectionnez **Signature électronique requise**.
   d. (Facultatif) Si des raisons prédéfinies sont requises, sélectionnez **N'utiliser que le motif prédéfini** et définissez les raisons.
8. Vérifiez que la case **Audité** est décochée pour les événements qui ne seront pas audités.
9. Cliquez sur **Enregistrer le modèle**.
   Le système invite l'utilisateur à appliquer la nouvelle carte à des projets.
10. Effectuez l'une des opérations suivantes :
    - Pour appliquer la nouvelle carte à des projets, cliquez sur **Oui**, sélectionnez les projets qui utiliseront cette nouvelle carte, puis cliquez sur **Appliquer**.

- Si vous ne souhaitez pas appliquer la nouvelle carte à des projets existants, cliquez sur **Non**.

11. (Facultatif) Pour utiliser cette carte d'audit comme carte d'audit par défaut pour tous les nouveaux projets, cliquez sur **Utiliser par défaut pour les nouveaux projets**.

Modifier une carte d'audit de projet

Remarque : Les modèles de cartes d'audit installés ne peuvent pas être édités.

1. Ouvrez l'espace de travail Configuration.
2. Cliquez sur **Cartes d'audit**.
3. Ouvrez l’onglet Modèles de projet.
4. Dans le champ **Modifier le modèle de carte**, sélectionnez la carte à modifier.
5. Sélectionnez et configurez les événements à enregistrer en respectant la procédure suivante :
   a. Cochez la case **Audité** pour l'événement.
   b. (Facultatif) Si une raison est requise, sélectionnez **Motif requis**.
   c. (Facultatif) Si une signature électronique est requise, sélectionnez **Signature électronique requise**.
   d. (Facultatif) Si des raisons prédéfinies sont requises, sélectionnez **N’utiliser que le motif prédéfini** et définissez les raisons.
6. Vérifiez que la case **Audité** est décochée pour les événements qui ne seront pas audités.
7. Cliquez sur **Enregistrer le modèle**.
   Le système invite l'utilisateur à appliquer la nouvelle carte à des projets.
8. Effectuez l'une des opérations suivantes :
   - Pour appliquer la nouvelle carte à des projets, cliquez sur **Oui**, sélectionnez les projets qui utiliseront cette nouvelle carte, puis cliquez sur **Appliquer**.
   - Si vous ne souhaitez pas appliquer la nouvelle carte à des projets existants, cliquez sur **Non**.

Modifier la carte d'audit active d'un projet

Quand une carte d'audit est appliquée au projet, elle devient la carte d'audit active. La configuration de l'audit dans la carte d'audit active détermine quels événements sont enregistrés dans les registres d'audit.

1. Ouvrez l'espace de travail Configuration.
2. Cliquez sur **Cartes d'audit**.
3. Ouvrez l’onglet Modèles de projet.

4. Dans le champ **Modifier le modèle de carte**, sélectionnez la carte d'audit à attribuer au projet.
5. Cliquez sur **Appliquer aux projets existants**.
   La boîte de dialogue Appliquer le modèle de carte d'audit du projet s'ouvre.
6. Cochez les cases correspondant aux projets auxquels appliquer cette carte d'audit.
7. Cliquez sur **Appliquer**.

Supprimer une carte d'audit de projet

Remarque : Les modèles de cartes d'audit installés ne peuvent pas être supprimés.

1. Ouvrez l'espace de travail Configuration.
2. Cliquez sur **Cartes d'audit**.
3. Ouvrez l'onglet Modèles de projet.
4. Dans le champ **Modifier le modèle de carte**, sélectionnez la carte à supprimer.
5. Cliquez sur **Supprimer un modèle**.
   Le système demande votre confirmation.
6. Cliquez sur **Oui**.

Cartes d'audit de poste de travail

Les cartes d'audit de poste de travail contrôlent l'audit des événements du poste de travail. Pour obtenir la liste des événements du poste de travail pouvant être audités, consultez la section Registre d'audit du poste de travail.

Créer une carte d'audit de poste de travail

1. Ouvrez l'espace de travail Configuration.
2. Cliquez sur **Cartes d'audit**.
3. Ouvrez l'onglet Modèles de poste de travail.
4. Dans le champ **Modifier le modèle de carte**, sélectionnez un modèle à utiliser comme base de la nouvelle carte.
5. Cliquez sur **Ajouter un modèle** ().
   La boîte de dialogue Ajouter un modèle de carte d'audit de poste de travail s'ouvre.
6. Cliquez sur le nom de la nouvelle carte, puis sur **OK**.
7. Sélectionnez et configurez les événements à enregistrer en respectant la procédure suivante :
   a. Cochez la case **Audité** pour l'événement.
   b. (Facultatif) Si une raison est requise, sélectionnez **Motif requis**.

c. (Facultatif) Si une signature électronique est requise, sélectionnez **Signature électronique requise**.

d. (Facultatif) Si des raisons prédéfinies sont requises, sélectionnez **N'utiliser que le motif prédéfini** et définissez les raisons.

8. Vérifiez que la case **Audité** est décochée pour les événements qui ne seront pas audités.
9. Cliquez sur **Enregistrer le modèle**.
10. (Facultatif) Pour utiliser cette carte d'audit comme carte d'audit active du poste de travail, cliquez sur **Appliquer au poste de travail**.

Modifier une carte d'audit de poste de travail

Remarque : Les modèles de cartes d'audit installés ne peuvent pas être édités.

1. Ouvrez l'espace de travail Configuration.
2. Cliquez sur **Cartes d'audit**.
3. Ouvrez l'onglet Modèles de poste de travail.
4. Dans le champ **Modifier le modèle de carte**, sélectionnez la carte à modifier.
5. Sélectionnez et configurez les événements à enregistrer en respectant la procédure suivante :

   a. Cochez la case **Audité** pour l'événement.

   b. (Facultatif) Si une raison est requise, sélectionnez **Motif requis**.

   c. (Facultatif) Si une signature électronique est requise, sélectionnez **Signature électronique requise**.

   d. (Facultatif) Si des raisons prédéfinies sont requises, sélectionnez **N'utiliser que le motif prédéfini** et définissez les raisons.

6. Vérifiez que la case **Audité** est décochée pour les événements qui ne seront pas audités.
7. Cliquez sur **Enregistrer le modèle**.
8. (Facultatif) Pour utiliser cette carte d'audit comme carte d'audit active du poste de travail, cliquez sur **Appliquer au poste de travail**.

Modifier la carte d'audit active d'un poste de travail

Quand une carte d'audit est appliquée au poste de travail, elle devient la carte d'audit active. La configuration de l'audit dans la carte d'audit active détermine quels événements sont enregistrés dans les registres d'audit.

1. Ouvrez l'espace de travail Configuration.
2. Cliquez sur **Cartes d'audit**.
3. Ouvrez l'onglet Modèles de poste de travail.

4. Dans le champ **Modifier le modèle de carte**, sélectionnez la carte à appliquer au poste de travail.
5. Cliquez sur **Appliquer au poste de travail**.

Supprimer une carte d'audit de poste de travail

Remarque : Les modèles de cartes d'audit installés ne peuvent pas être supprimés.

1. Ouvrez l'espace de travail Configuration.
2. Cliquez sur **Cartes d'audit**.
3. Ouvrez l'onglet Modèles de poste de travail.
4. Dans le champ **Modifier le modèle de carte**, sélectionnez la carte à supprimer.
5. Cliquez sur **Supprimer un modèle**.
   Le système demande votre confirmation.
6. Cliquez sur **Oui**.

Cartes d'audit CAC

Les cartes d'audit CAC contrôlent l'audit des événements du poste de travail CAC. Pour obtenir la liste des événements pouvant être audités, consultez la section Registre d'audit du poste de travail.

Créer une carte d’audit CAC

1. Ouvrez l'espace de travail Configuration.
2. Cliquez sur **Cartes d'audit**.
3. Ouvrez l'onglet Modèles CAC.
4. Dans le champ **Modifier le modèle de carte**, sélectionnez un modèle à utiliser comme base de la nouvelle carte.
5. Cliquez sur **Ajouter un modèle** ().
   La boîte de dialogue Ajouter un modèle de carte d’audit CAC s’ouvre.
6. Cliquez sur le nom de la nouvelle carte, puis sur **OK**.
7. Sélectionnez et configurez les événements à enregistrer en respectant la procédure suivante :
   a. Cochez la case **Audité** pour l'événement.
   b. (Facultatif) Si une raison est requise, sélectionnez **Motif requis**.
   c. (Facultatif) Si une signature électronique est requise, sélectionnez **Signature électronique requise**.
   d. (Facultatif) Si des raisons prédéfinies sont requises, sélectionnez **N’utiliser que le motif prédéfini** et définissez les raisons.

8. Vérifiez que la case **Audité** est décochée pour les événements qui ne seront pas audités.
9. Cliquez sur **Enregistrer le modèle**.
10. (Facultatif) Pour utiliser cette carte d'audit comme carte d'audit active du poste de travail CAC, cliquez sur **Appliquer au CAC**.

Modifier une carte d’audit CAC

Remarque : Les modèles de cartes d'audit installés ne peuvent pas être édités.

1. Ouvrez l'espace de travail Configuration.
2. Cliquez sur **Cartes d'audit**.
3. Ouvrez l'onglet Modèles CAC.
4. Dans le champ **Modifier le modèle de carte**, sélectionnez la carte à modifier.
5. Sélectionnez et configurez les événements à enregistrer en respectant la procédure suivante :
    a. Cochez la case **Audité** pour l'événement.
    b. (Facultatif) Si une raison est requise, sélectionnez **Motif requis**.
    c. (Facultatif) Si une signature électronique est requise, sélectionnez **Signature électronique requise**.
    d. (Facultatif) Si des raisons prédéfinies sont requises, sélectionnez **N’utiliser que le motif prédéfini** et définissez les raisons.
6. Vérifiez que la case **Audité** est décochée pour les événements qui ne seront pas audités.
7. Cliquez sur **Enregistrer le modèle**.
8. (Facultatif) Pour utiliser cette carte d'audit comme carte d'audit active du poste de travail CAC, cliquez sur **Appliquer au CAC**.

Modifier la carte d'audit active d’un système CAC

Quand une carte d'audit est appliquée au poste de travail CAC, elle devient la carte d'audit active. La configuration de l'audit dans la carte d'audit active détermine quels événements sont enregistrés dans les registres d'audit.

1. Ouvrez l'espace de travail Configuration.
2. Cliquez sur **Cartes d'audit**.
3. Ouvrez l'onglet Modèles CAC.
4. Dans le champ **Modifier le modèle de carte**, sélectionnez la carte à appliquer au poste de travail CAC.
5. Cliquez sur **Appliquer au CAC**.

Supprimer une carte d’audit CAC

Remarque : Les modèles de cartes d'audit installés ne peuvent pas être supprimés.

1. Ouvrez l'espace de travail Configuration.
2. Cliquez sur **Cartes d'audit**.
3. Ouvrez l'onglet Modèles CAC.
4. Dans le champ **Modifier le modèle de carte**, sélectionnez la carte à supprimer.
5. Cliquez sur **Supprimer un modèle**.
   Le système demande votre confirmation.
6. Cliquez sur **Oui**.

Afficher, rechercher, exporter et imprimer des registres d'audit

Cette section fournit des informations sur l'affichage des registres d'audit et des registres d'audit archivés. Elle aborde également les étapes nécessaires pour l'exportation, l'impression, la recherche et le tri des enregistrements d'audit dans les registres d'audit.

Afficher les enregistrements du registre d'audit

1. Ouvrez l'espace de travail Trace d'audit.
2. Dans le volet de gauche, cliquez sur le registre d'audit à visualiser.
3. Pour afficher les informations détaillées concernant un événement d'audit, cliquez sur l’événement en question.

   Le type d'événement sélectionné contrôle les informations affichées. Les informations s'affichent dans un ou plusieurs des onglets suivants.

Tableau 7-4 : Onglets Détails de l'événement

Onglet	Information
Détails généraux	Affiche des informations, comme le décalage du fuseau horaire et le nom du poste de travail.
Avant modification	Affiche le contenu avant la modification apportée.
Après modification	Affiche le contenu après la modification apportée.
Détails de la modification	Affiche le contenu d’origine et le nouveau contenu dans le même volet. Dans Vue Différence, le contenu d’origine s'affiche en rouge et le nouveau contenu en vert. Dans Vue Côte à côte, le contenu d’origine et le nouveau contenu s'affichent dans des volets différents, permettant à l'utilisateur d’identifier facilement les modifications.

Rechercher ou filtrer des enregistrements d'audit

1. Ouvrez l'espace de travail Trace d'audit.
2. Sélectionnez le registre d'audit à rechercher.
3. Pour rechercher un registre d'audit spécifique, entrez du texte dans le champ **Rechercher dans la page**.
   Toutes les occurrences du texte indiqué sur la page sont mises en surbrillance.
4. Pour filtrer les enregistrements du registre d'audit, suivez les étapes ci-après :
   a. Cliquez sur l'icône de filtre (entonnoir).
      La boîte de dialogue Filtrer le registre d'audit s'ouvre.
   b. Tapez les critères de filtre.
   c. Cliquez sur **OK**.

Afficher un registre d'audit archivé

Lorsqu'un registre d'audit contient 20 000 enregistrements, le logiciel SCIEX OS les archive automatiquement et enregistre les suivants dans un nouveau registre. Les noms de fichier de registre d'audit archivés indiquent le type de registre d'audit ainsi que la date et l'heure. Par exemple, le nom de fichier pour une archive de registre d'audit de poste de travail est au format `WorkstationAuditTrailData-<workstation name>>-<YYYY><MMDDHHMMSS>.atds`.

Cette procédure peut également être utilisée pour ouvrir un registre d'audit pour un tableau de résultats.

1. Ouvrez l'espace de travail Trace d'audit.
2. Cliquez sur **Parcourir**.
3. Accédez à et sélectionnez le registre d'audit archivé à ouvrir, puis cliquez sur **OK**.

Remarque : Pour ouvrir le registre d'audit d'un tableau de résultats, sélectionnez le fichier `qsession` associé.

Imprimer un registre d'audit

1. Ouvrez l'espace de travail Trace d'audit.
2. Sélectionnez le registre d'audit à imprimer.
3. Cliquez sur **Imprimer**.
   La boîte de dialogue Imprimer s'ouvre.
4. Sélectionnez l'imprimante et cliquez sur **OK**.

Exporter les enregistrements du registre d'audit

1. Ouvrez l'espace de travail Trace d'audit.
2. Sélectionnez le registre d'audit à exporter.

3. Cliquez sur **Exporter**.
4. Accédez à l'emplacement de stockage du fichier exporté, entrez un **Nom de fichier** puis cliquez sur **Enregistrer**.
   Le registre d'audit est sauvegardé dans un fichier à valeurs séparées par une virgule (csv).

Enregistrements de registre d'audit SCIEX OS

Cette section décrit les champs dans les enregistrements dans le registre d'audit.

Les registres d'audit du poste de travail et du projet sont des fichiers chiffrés.

Remarque : Les registres d'audit et les archives du poste de travail sont conservés dans le dossier `Program Data\SCIEX\Audit Data`. Les registres d'audit et les archives du projet sont stockés dans le dossier `Audit Data` du projet.

Tableau 7-5 : Champs d'enregistrement d'audit

Libellé	Description
Horodatage	La date et l'heure de création de l'enregistrement.
Nom de l'événement	Le nom de l'événement.
Description	La description de l'événement.
Motif	La raison donnée pour l'événement.
Signature électronique	Indique si une signature électronique a été entrée pour l'événement.
Nom d'utilisateur complet	Le nom de l'utilisateur. **Remarque :** Pour les événements déclenchés par une règle de décision, c'est l'utilisateur qui a soumis le lot.
Utilisateur	L'ID de l'utilisateur qui a initié l'événement à l'origine de l'enregistrement.
Catégorie	La fonction ou catégorie à laquelle appartient l'événement.

La partie inférieure de l'espace de travail Trace d'audit affiche des informations sur un événement sélectionné, notamment les modifications apportées le cas échéant.

Vous trouverez les listes des événements enregistrés dans les registres d'audit de projet et de la station de travail dans les sections Registre d'audit du poste de travail et Registre d'audit du projet.

Enregistrements de registre d'audit CAC

Cette section décrit les champs dans les enregistrements dans le registre d'audit.

Les registres d'audit de CAC et de projet sont des fichiers chiffrés.

Remarque : Les registres d'audit et les archives de CAC sont conservés dans le dossier `Program Data\SCIEX\Audit Data`. Les registres d'audit et les archives du projet sont stockés dans le dossier `Audit Data` du projet.

Tableau 7-6 : Champs d'enregistrement d'audit

Libellé	Description
Horodatage	La date et l'heure de création de l'enregistrement.
Nom de l'événement	Le nom de l'événement.
Description	La description de l'événement.
Motif	La raison donnée pour l'événement.
Signature électronique	Indique si une signature électronique a été entrée pour l'événement.
Nom d'utilisateur complet	Le nom de l'utilisateur. **Remarque :** Pour les événements déclenchés par une règle de décision, c'est l'utilisateur qui a soumis le lot.
Utilisateur	L'ID de l'utilisateur qui a initié l'événement à l'origine de l'enregistrement.
Catégorie	La fonction ou catégorie à laquelle appartient l'événement.

La partie inférieure de l'espace de travail Trace d'audit affiche des informations sur un événement sélectionné, notamment les modifications apportées le cas échéant.

Pour une liste des événements enregistrés dans les registres d'audit de CAC et de projet, consultez les sections Tableau 3 et Registre d'audit du projet.

Archives de registres d'audit

Les registres d'audit s'accumulent dans le registre d'audit du projet et dans le registre d'audit du poste de travail et peuvent créer des fichiers volumineux difficiles à visualiser et à gérer.

Lorsqu'un registre d'audit atteint 20 000 enregistrements, il est archivé. Un enregistrement d'archive final est ajouté au registre d'audit, qui est alors sauvegardé sous un nom indiquant le type de registre d'audit ainsi que la date et l'heure. Un nouveau registre d'audit est créé. Le premier enregistrement du nouveau registre d'audit indique que le registre d'audit a été archivé et spécifie le chemin vers le registre d'audit archivé.

Les archives du registre d'audit de poste de travail sont stockées dans le dossier `C:\ProgramData\SCIEX\Audit Data`. Les noms de fichiers sont au format WorkstationAuditTrailData-*<nom du poste de travail>*-*<AAAA><MMJJHHMMSS>*.atds. Par exemple, `WorkstationAuditTrailData-SWDSXPT158-20190101130401.atds`.

Les archives du registre d'audit du projet sont stockées dans le dossier `Audit Data` du projet.

Accéder aux données pendant des interruptions du réseau A

Afficher et traiter des données localement

En cas d'interruption temporaire du réseau au cours d'une acquisition réseau, les données acquises sont accessibles dans le dossier `NetworkBackup` sur l'ordinateur d'acquisition. Pour éviter toute altération des données, il est recommandé de copier les fichiers de données contenus dans le dossier `NetworkBackup` vers un nouvel emplacement avant de les afficher ou de les traiter, et de conserver l'exemplaire original des fichiers dans le dossier `NetworkBackup`.

Toutes les 15 minutes, le logiciel SCIEX OS détermine si l'emplacement réseau est disponible. S'il l'est, le transfert des données reprend.

Le dossier `NetworkBackup` est stocké dans le répertoire racine local, généralement `D:\SCIEX OS Data\NetworkBackup`. Les fichiers de données de chaque lot sont stockés dans un dossier dont le nom est un identifiant unique. L'estampille temporelle des dossiers indique la date et l'heure de début de lot et peut servir à identifier le dossier qui contient les données souhaitées.

Retirer des échantillons des dossiers de transfert réseau

Si la connectivité réseau est perdue pendant une période prolongée ou si le répertoire racine du réseau est modifié, il peut être nécessaire de supprimer des fichiers de données des dossiers de transfert réseau. Nous recommandons que cette action soit effectuée par un administrateur système possédant d'excellentes compétences techniques en matière de réseaux.

1. Ouvrez l'espace de travail File d'attente.
2. Arrêtez la file d'attente.
3. Annulez tous les échantillons restants dans le lot qui contient les échantillons à supprimer.
4. Fermez le logiciel SCIEX OS.
5. Arrêtez **Clearcore2.Service.exe**.

   Conseil ! Exécutez cette tâche depuis le Gestionnaire des services de Windows.

6. Déplacez temporairement vers un autre dossier tous les fichiers et dossiers dans les dossiers `OutBox` et `NetworkBackup` en attente de transfert vers le répertoire racine indisponible. Ne supprimez pas les dossiers `OutBox` ou `NetworkBackup`.

Remarque : Le dossier `OutBox` est un dossier masqué dans le répertoire racine local, généralement `D:\SCIEX OS Data\TempData\Outbox`. Lorsque les fichiers et les dossiers dans `Outbox` ne sont plus nécessaires, ils peuvent être supprimés.

ATTENTION : Risque de perte de données. Ne supprimez pas le fichier si les données contenues dans l'échantillon bloqué doivent être conservées.

7. Ouvrez le logiciel SCIEX OS.
   Dans un délai de 15 minutes, le logiciel SCIEX OS tente de se connecter à la ressource réseau. Si la connexion aboutit, le transfert reprend. Lorsque le transfert est terminé, les dossiers contenus dans le dossier `NetworkBackup` sont supprimés.

Autorisations de Windows B

Cette section fournit une liste des autorisations de Windows requises pour chaque rôle d'utilisateur et l'utilisateur SYSTEM, pour le fonctionnement correct du logiciel SCIEX OS.

Remarque : Le chemin d'accès par défaut du dossier *Installed Root Directory* est `D:\SCIEX OS Data`.

Tableau B-1 : *Installed Root Directory* Dossier

Autorisation	Administrateur, SYSTEM	Analyste, Développeur de méthode, Vérificateur
Contrôle total	Autoriser	—
Parcourir le dossier / Exécuter le fichier	Autoriser	Autoriser
Lister le dossier / Lire les données	Autoriser	Autoriser
Lire les attributs	Autoriser	Autoriser
Lire les attributs étendus	Autoriser	Autoriser
Créer des fichiers / Écrire des données	Autoriser	Autoriser
Créer des dossiers / Ajouter des données à la fin	Autoriser	Autoriser
Écrire des attributs	Autoriser	Autoriser
Écrire des attributs étendus	Autoriser	Autoriser
Supprimer des sous-dossiers et des fichiers	Autoriser	—
Supprimer	Autoriser	—
Lire les autorisations	Autoriser	Autoriser

Tableau B-1 : *Installed Root Directory* Dossier (suite)

Autorisation	Administrateur, SYSTEM	Analyste, Développeur de méthode, Vérificateur
Modifier les autorisations	Autoriser	—
S'approprier	Autoriser	—

Tableau B-2 : Dossiers *`Installed Root Directory`*`\NetworkBackup` et *`Installed Root Directory`*`\TempData`

Autorisation	Administrateur, SYSTEM	Analyste, Développeur de méthode, Vérificateur
Contrôle total	Autoriser	—
Parcourir le dossier / Exécuter le fichier	Autoriser	Autoriser
Lister le dossier / Lire les données	Autoriser	Autoriser
Lire les attributs	Autoriser	Autoriser
Lire les attributs étendus	Autoriser	Autoriser
Créer des fichiers / Écrire des données	Autoriser	Autoriser
Créer des dossiers / Ajouter des données à la fin	Autoriser	Autoriser
Écrire des attributs	Autoriser	Autoriser
Écrire des attributs étendus	Autoriser	Autoriser
Supprimer des sous-dossiers et des fichiers	Autoriser	Autoriser
Supprimer	Autoriser	Autoriser
Lire les autorisations	Autoriser	Autoriser

Tableau B-2 : Dossiers *Installed Root Directory*\NetworkBackup et *Installed Root Directory*\TempData (suite)

Autorisation	Administrateur, SYSTEM	Analyste, Développeur de méthode, Vérificateur
Modifier les autorisations	Autoriser	—
S'approprier	Autoriser	—

Tableau B-3 : Dossier C:\ProgramData\SCIEX\Audit Data

Autorisation	Administrateur, SYSTEM	Analyste, Développeur de méthode, Vérificateurs
Contrôle total	Autoriser	—
Parcourir le dossier / Exécuter le fichier	Autoriser	Autoriser
Lister le dossier / Lire les données	Autoriser	Autoriser
Lire les attributs	Autoriser	Autoriser
Lire les attributs étendus	Autoriser	Autoriser
Créer des fichiers / Écrire des données	Autoriser	Autoriser
Créer des dossiers / Ajouter des données à la fin	Autoriser	Autoriser
Écrire des attributs	Autoriser	Autoriser
Écrire des attributs étendus	Autoriser	Autoriser
Supprimer des sous-dossiers et des fichiers	Autoriser	—
Supprimer	Autoriser	—
Lire les autorisations	Autoriser	Autoriser

Tableau B-3 : Dossier `C:\ProgramData\SCIEX\Audit Data` (suite)

Autorisation	Administrateur, SYSTEM	Analyste, Développeur de méthode, Vérificateurs
Modifier les autorisations	Autoriser	—
S’approprier	Autoriser	—

Événements d'audit C

Cette section répertorie les événements d'audit dans SCIEX OS. Elle répertorie également les événements d'audit correspondants dans le logiciel Analyst, pour les utilisateurs qui migrent du logiciel Analyst vers SCIEX OS.

Registre d'audit du projet

Chaque projet possède un registre d'audit de projet. Le registre d'audit du projet est stocké dans le dossier `Audit Data` du projet. Le nom de fichier du registre d'audit est `ProjectAuditEvents.atds`.

Remarque : La carte d'audit par défaut des nouveaux projets créés dans le logiciel Central Administrator Console (CAC) est la Carte d'audit silencieuse.

Les événements du registre d'audit de projet sont affichés dans le logiciel CAC et SCIEX OS.

Tableau C-1 : Événements du registre d'audit de projet

SCIEX OS ou CAC	Logiciel Analyst
Espace de travail Analytics	
Concentration réelle modifiée	Événements de quantification : **'Concentration' has been changed**
Fichier de traitement automatique enregistré	—
ID du code-barres modifié	—
Échantillon de comparaison modifié dans le flux de travail non ciblé	—
Colonnes personnalisées modifiées	Événements de quantification : **'Custom Title' has changed**
Exploration des données ouverte	Événements de projet : **Data File has been opened**
Données exportées	—
Données transférées au LIMS	—
Facteur de dilution modifié	Événements de quantification : **'Dilution Factor' has been changed**
Étalonnage externe modifié	—
Étalonnage externe exporté	—

Tableau C-1 : Événements du registre d'audit de projet (suite)

SCIEX OS ou CAC	Logiciel Analyst
Fichier enregistré	Événements de projet : **Quantitation Results Table has been created**, **Quantitation Results Table has been modified**, événements de quantification : **Results Table has been saved**
Colonne de formule modifiée	Événements de quantification : **Formula name has been changed**, **Formula name has been added**, **Formula string has been changed**, **Formula column has been removed**
Intégration effacée	—
Paramètres d'intégration modifiés	Événements de quantification : **Quantitation peak has been integrated**
Résultat de la recherche en bibliothèque modifié	—
Intégration manuelle	Événements de quantification : **Quantitation Peak has been integrated**
Intégration manuelle inversée	Événements de quantification : **Quantitation peak has been reverted back to original**
Sélection MS/MS modifiée	—
Méthode de traitement modifiée et appliquée	Événements de quantification : **Quantitation method has been changed**
Méthode de traitement enregistrée	—
Paramètres par défaut du projet modifiés	—
Rapport créé	Événements de projet : **Printing document on printer, Finished printing document on printer**
Tableau de résultats approuvé	Événements de quantification : **QA reviewer has accessed a results table**
Tableau de résultats créé	Événements de quantification : **Results table has been created**
Tableau de résultats verrouillé	—
Tableau de résultats déverrouillé	—
ID d'échantillon modifié	Événements de quantification : **'Sample ID' has been changed**

Tableau C-1 : Événements du registre d'audit de projet (suite)

SCIEX OS ou CAC	Logiciel Analyst
Nom d'échantillon modifié	Événements de quantification : **'Sample Name' has been changed**
Type d'échantillon modifié	Événements de quantification : **'Sample Type' has been changed**
Échantillons ajoutés ou supprimés	Événements de quantification : **Files have been added to Results Table**, **Files have been removed from Results Table**, **Samples have been added/removed**
Concentration réelle de l'ajout de standard modifiée	—
Sélection modifiée des colonnes utilisées	Événements de quantification : **'Use IT' has been changed**
Poids/Volume modifié	**'Weight to Volume Ratio' has been changed**
Fenêtre/volet imprimé(e)	Événements de projet : **Printing document on printer**, **Finished printing document on printer**
Page Carte d'audit	
Carte d'audit de projet modifiée	Événements de projet : **Project Settings have been changed**
Trace d'audit de projet exportée	—
Trace d'audit de projet imprimée	—
Espace de travail Lot	
Informations de lot importées depuis LIMS/texte	—
Lot enregistré	—
Lot envoyé	Événements d'instrument : **Batch file submitted**
Imprimer	Événements de projet : **Printing Document on printer**, **Finished printing document on printer**
Espace de travail Explorateur[4]	
Ouvrir échantillon(s)	Événements de projet : **Data File has been opened**

[4] Les événements Explorateur sont enregistrés dans le registre d'audit du projet lorsque des utilisateurs utilisent des données du projet actif.

Tableau C-1 : Événements du registre d'audit de projet (suite)

SCIEX OS ou CAC	Logiciel Analyst
Imprimer	Événements de projet : **Printing Document on printer**, **Finished printing document on printer**
Réétalonnage d'échantillon(s)	—
Réétalonnage d'échantillon(s) commencé	—
Espace de travail Méthode LC	
Méthode LC enregistrée	—
Imprimer	Événements de projet : **Printing Document on printer**, **Finished printing document on printer**
Espace de travail Méthode MS	
Méthode MS enregistrée	—
Imprimer	Événements de projet : **Printing Document on printer**, **Finished printing document on printer**
Espace de travail File d'attente	
L'acquisition de l'échantillon est terminée	—
Échantillon modifié	—
Début d'acquisition de l'échantillon	—
Échantillon transféré	—

Registre d'audit du poste de travail

Chaque poste de travail possède un registre d'audit de poste de travail. Le registre d'audit du poste de travail est stocké dans le dossier `Program Data\SCIEX\Audit Data`. Le nom de fichier du registre d'audit est au format : `WorkstationAuditTrailData.atds`.

Remarque : La carte d'audit par défaut pour les nouveaux postes de travail dans le logiciel Central Administrator Console (CAC) est **Carte d'audit silencieuse**.

Les événements du registre d'audit sont affichés dans le logiciel CAC et SCIEX OS.

Tableau C-2 : Événements du registre d'audit du poste de travail

SCIEX OS	Logiciel Analyst
Carte d'audit	

Tableau C-2 : Événements du registre d'audit du poste de travail (suite)

SCIEX OS	Logiciel Analyst
Carte d'audit de poste de travail modifiée	Événements d'instrument : **Instrument Settings have been changed**
Trace d'audit de poste de travail imprimée	—
Trace d'audit de poste de travail exportée	—
CAC	
Administration centrale activée/ désactivée	—
Paramètres d'Administration centrale récupérés/impossibles à récupérer	—
Somme de contrôle du fichier de données	
La somme de contrôle du fichier de données wiff a été modifiée	—
Espace de travail Explorateur[5]	
Ouvrir échantillon(s)	Événements de projet : **Data File has been opened**
Imprimer	Événements de projet : **Printing document on printer**, **Finished printing document on printer**
Réétalonnage d'échantillon(s)	—
Réétalonnage d'échantillon(s) commencé	—
Configuration matérielle	
Appareils activés	Événements d'instrument : **Hardware profile has been activated**
Appareils désactivés	Événements d'instrument : **Hardware profile has been deactivated**
Réglage de l'instrument	
Mise à jour du réglage automatique du SM	Événements d'instrument : **Tune parameter settings changed**
Micrologiciel modifié	—
Modification des réglages du SM	Événements d'instrument : **Tune parameter settings changed**

[5] Les événements Explorateur sont enregistrés dans le registre d'audit du poste de travail lorsque des utilisateurs utilisent des projets qui ne sont pas dans le projet actif.

Tableau C-2 : Événements du registre d'audit du poste de travail (suite)

SCIEX OS	Logiciel Analyst
Imprimer le résultat de la procédure dans MS Tune	Événements de projet : **Printing Document on printer**, **Finished printing document on printer**
Espace de travail File d'attente	
Une injection automatique a été effectuée	—
Une réinjection automatique a été effectuée	—
Lot déplacé dans la file d'attente	Événements d'instrument : **Move Batch**
File d'attente d'impression	Événements de projet : **Printing Document on printer**, **Finished printing document on printer**
Nouvelle acquisition de l'échantillon	Événements d'instrument : **Reacquiring sample(s)**
L'acquisition de l'échantillon est terminée	Événements de projet : **Sample has been added to Data file**
Échantillon modifié	—
Échantillon déplacé dans la file d'attente	Événements d'instrument : **Sample moved from position *x* to position *y* of Batch File**
Début d'acquisition de l'échantillon	—
Sécurité	
Déconnexion automatique par le système	Événements d'instrument : **User Logged out**
Déconnexion forcée par un autre utilisateur	Événements d'instrument : **User Logged out**
Échec de la déconnexion forcée	—
Échec du déverrouillage de l'écran	—
Les identifiants de compte réseau sécurisé ont été modifiés	Événements d'instrument : **Acquisition Account Changed**
Les identifiants de compte réseau sécurisé ont été supprimés.	Événements d'instrument : **Acquisition Account Changed**
Les identifiants de compte réseau sécurisé ont été spécifiés.	Événements d'instrument : **Acquisition Account Changed**
Configuration de sécurité modifiée	Événements d'instrument : **The Security Configuration has been modified**, **Screen Lock Changed**, **Auto Logout changed**

Tableau C-2 : Événements du registre d'audit du poste de travail (suite)

SCIEX OS	Logiciel Analyst
Utilisateur ajouté/supprimé	Événements d'instrument : **User Added**, **User Deleted**
L'utilisateur s'est connecté	Événements d'instrument : **User Logged In**
L'utilisateur s'est déconnecté	Événements d'instrument : **User Logged out**
L'utilisateur a désactivé le mode exclusif	—
Échec de connexion de l'utilisateur	Événements d'instrument : **User Login Failed**
Les paramètres de gestion des utilisateurs ont été exportés	—
Les paramètres de gestion des utilisateurs ont été importés	—
Les paramètres de gestion des utilisateurs ont été rétablis	—
Rôle attribué à l'utilisateur/au groupe d'utilisateurs	Événements d'instrument : **User Changed User Type**
Rôle utilisateur supprimé	Événements d'instrument : **User Type Deleted**
Rôle utilisateur modifié	Événements d'instrument : **User Type Changed**
Journal des utilisateurs	
Imprimer le registre d'événements	—

Tableau C-3 : Événements du registre d'audit de CAC

CAC	Logiciel Analyst
Page Carte d'audit	
Carte d'audit de poste de travail modifiée	Événements d'instrument : **Instrument Settings have been changed**
Trace d'audit de poste de travail imprimée	—
Trace d'audit de poste de travail exportée	—
CAC	
Les paramètres de CAC ont été exportés	—
Les paramètres de CAC ont été importés	—

Tableau C-3 : Événements du registre d'audit de CAC (suite)

CAC	Logiciel Analyst
Les paramètres de CAC ont été restaurés	—
Paramètres de projet activés/désactivés dans un groupe de travail	—
Projets affectés à/dissociés d'un groupe de travail	—
Autorisation de sécurité ajoutée pour l'administration centrale	—
Utilisateur ajouté/supprimé	—
Rôle utilisateur ajouté	—
Rôle utilisateur supprimé	—
Rôle utilisateur modifié	—
Rôle(s) utilisateur associé(s)/dissocié(s) à un/des utilisateur(s) dans le groupe de travail	—
Utilisateur(s)/Groupe(s) d'utilisateurs associé(s) à un groupe de travail ou dissocié(s) d'un groupe de travail	—
Groupe de travail ajouté/supprimé	—
Groupe de travail renommé	—
Poste(s) de travail associé(s) à/ dissocié(s) d'un groupe de travail	—
Sécurité	
Déconnexion automatique par le système	Événements d'instrument : **User Logged out**
Déconnexion forcée par un autre utilisateur	Événements d'instrument : **User Logged out**
Échec de la déconnexion forcée	—
Échec du déverrouillage de l'écran	—
Les identifiants de compte réseau sécurisé ont été modifiés	Événements d'instrument : **Acquisition Account Changed**
Les identifiants de compte réseau sécurisé ont été supprimés.	Événements d'instrument : **Acquisition Account Changed**
Les identifiants de compte réseau sécurisé ont été spécifiés.	Événements d'instrument : **Acquisition Account Changed**

Tableau C-3 : Événements du registre d'audit de CAC (suite)

CAC	Logiciel Analyst
Configuration de sécurité modifiée	Événements d'instrument : **The Security Configuration has been modified**, **Screen Lock Changed**, **Auto Logout changed**
Utilisateur ajouté/supprimé	Événements d'instrument : **User Added**, **User Deleted**
L'utilisateur s'est connecté	Événements d'instrument : **User Logged In**
L'utilisateur s'est déconnecté	Événements d'instrument : **User Logged out**
L'utilisateur a désactivé le mode exclusif	—
Échec de connexion de l'utilisateur	Événements d'instrument : **User Login Failed**
Les paramètres de gestion des utilisateurs ont été exportés	—
Les paramètres de gestion des utilisateurs ont été importés	—
Les paramètres de gestion des utilisateurs ont été rétablis	—
Rôle attribué à l'utilisateur/au groupe d'utilisateurs	Événements d'instrument : **User Changed User Type**
Rôle utilisateur supprimé	Événements d'instrument : **User Type Deleted**
Rôle utilisateur modifié	Événements d'instrument : **User Type Changed**
Journal des utilisateurs	
Imprimer le registre d'événements	—

Mappage des autorisations entre les logiciels SCIEX OS et Analyst D

Cette section s'adresse aux utilisateurs qui ont besoin de migrer leurs paramètres de sécurité lors de la migration du logiciel Analyst vers le logiciel SCIEX OS. Elle montre les autorisations du logiciel Analyst, qui correspondent aux autorisations du logiciel SCIEX OS.

Tableau D-1 : Mappage des autorisations

Logiciel SCIEX OS	Logiciel Analyst
Espace de travail Lot	
Envoyer les méthodes déverrouillées	—
Ouvrir	Lot : **Open Existing Batches**
Enregistrer sous	Lot : **Create New Batches**, **Import**, **Edit Batches**, **Save Batches**, **Overwrite Batches**
Envoyer	Lot : **Submit Batches**
Enregistrer	Lot : **Save Batches**, **Overwrite Batches**
Enregistrer le tableau de référence d'ions	—
Ajouter des sous-dossiers de données	—
Configurer les règles de décision	—
Espace de travail Configuration	
Onglet Général	—
Général : modifier le paramètre régional	—
Général : mode plein écran	—
Général : arrêter les services Windows	—
Onglet Communication LIMS	—
Onglet Cartes d'audit	Gestionnaire de registre d'audit : **Change Audit Trail Settings**, **Create or Modify Audit Maps**
Onglet File d'attente	—
File d'attente : période d’inactivité de l’instrument	—
File d'attente : nombre max. d'échantillons acquis	—

Tableau D-1 : Mappage des autorisations (suite)

Logiciel SCIEX OS	Logiciel Analyst
File d'attente : autres paramètres de file d'attente	—
Onglet Projets	—
Projets : créer un projet	Application Analyst : **Create Project**
Projets : appliquer un modèle de carte d'audit à un projet	Gestionnaire de registre d'audit : **Change Audit Trail Settings**
Projets : créer le répertoire racine	Application Analyst : **Create Root Directory**
Projet : définir le répertoire racine actuel	Application Analyst : **Set Root Directory**
Projets : spécifier les identifiants réseau	—
Projets : activer l'écriture de somme de contrôle pour la création de données wiff	—
Projets : effacer le répertoire racine	—
Onglet Appareils	Configuration matérielle : **Create**, **Delete**, **Edit**, **Activate/Deactivate**
Onglet Gestion des utilisateurs	**Security Config**
Forcer la déconnexion de l'utilisateur	**Unlock/Logout Application**
Onglet CAC[3]	—
Onglet Modèles d'impression	—
Modèles d'impression : Créer et modifier des modèles d'impression	—
Modèles d'impression : Définir le modèle d'impression par défaut	—
Modèles d'impression : Appliquer le modèle actuel à tous les projets du répertoire racine	
Espace de travail Registre d'événements	
Accéder à l'espace de travail Registre d'événements	—
Registre d'archive	—
Espace de travail Trace d'audit	

[3] Dans la version 3.1, l'autorisation **Activer Central Administration** a été renommée en **CAC**. La page CAC dans l'espace de travail Configuration permet de configurer l'administration centrale du logiciel SCIEX OS.

Tableau D-1 : Mappage des autorisations (suite)

Logiciel SCIEX OS	Logiciel Analyst
Accéder à l'espace de travail Trace d'audit	Gestionnaire de registre d'audit : **View Audit Trail Data**
Afficher la carte d'audit active	Gestionnaire de registre d'audit : **View Audit Trail Data**
Imprimer/exporter la trace d'audit	Gestionnaire de registre d'audit : **View Audit Trail Data**
Data Acquisition Panel	
Démarrage	—
Arrêter	—
Enregistrer	—
Espaces de travail Méthode MS et Méthode LC	
Accéder à l'espace de travail Méthode	—
Nouveau	Méthode d'acquisition : **Create/Save acquisition method**
Ouvrir	Méthode d'acquisition : **Open acquisition method as read-only (acquire mode)**
Enregistrer	Méthode d'acquisition : **Overwrite acquisition methods**, **Create/Save acquisition method**
Enregistrer sous	Méthode d'acquisition : **Overwrite acquisition methods**, **Create/Save acquisition method**
Verrouiller/déverrouiller la méthode	—
Espace de travail File d'attente	
Gérer	File d'attente d'échantillons : **Reacquire**, **Delete Sample or Batch**, **Move Batch**
Démarrer/Arrêter	File d'attente d'échantillons : **Start Sample**, **Stop Sample**, **Abort Sample**, **Stop Queue**
Imprimer	Éditeur de modèle de rapport : **Print**
Modifier l'échantillon	—
Espace de travail Bibliothèque	

Tableau D-1 : Mappage des autorisations (suite)

Logiciel SCIEX OS	Logiciel Analyst
Accéder à l'espace de travail Bibliothèque	Explorer : **Setup library location**, **Setup library user options**, **Add library record**, **Add spectrum to library**, **Modify library record (overrides add/delete if disabled)**, **Delete MS spectrum**, **Delete UV spectrum**, **Delete structure**, **View library**, **Search library**
Espace de travail Réglage MS	
Accéder à l'espace de travail Réglage MS	—
Réglage MS avancé	Régler : **Instrument Optimization**, **Manual Tune**, **Edit Tuning Options**
Dépannage avancé	—
Vérification d'état rapide	Régler : **Instrument Opt**
Restaurer les données de l'instrument	Régler : **Edit Tuning Options**, **Edit instrument data**
Espace de travail Explorateur	
Accéder à l'espace de travail Explorateur	—
Exporter	Explorer : **Save data to text file**
Imprimer	Éditeur de modèle de rapport : **Print**
Options	—
Réétalonner	Régler : **Calibrate from current spectrum**
Espace de travail Analytics	
Nouveaux résultats	Quantification : **Create new results tables**
Créer une méthode de traitement	Quantification : **Create quantitation methods**
Modifier la méthode de traitement	Quantification : **Modify existing methods**
Autoriser l'exportation et la création d'un rapport du tableau de résultats déverrouillé	—
Enregistrer les résultats pour le lot d'automatisation	—
Modifier l'algorithme d'intégration de la méthode de quantification par défaut	Quantification : **Change default method options**
Modifier les paramètres d'intégration de la méthode de quantification par défaut	Quantification : **Change default method options**

Tableau D-1 : Mappage des autorisations (suite)

Logiciel SCIEX OS	Logiciel Analyst
Activer l'avertissement de pic modifié du projet	—
Ajouter des échantillons	Quantification : **Add and Remove samples from results table**
Supprimer les échantillons sélectionnés	Quantification : **Add and Remove samples from results table**
Exporter, importer ou supprimer un étalonnage externe	—
Modifier le nom de l'échantillon	Quantification : **Modify sample name**
Modifier le type d'échantillon	Quantification : **Modify Sample Type**
Modifier l'ID d'échantillon	Quantification : **Modify Sample ID**
Modifier la concentration réelle	Quantification : **Modify Analyte Concentration**
Modifier le facteur de dilution	Quantification : **Modify Dilution Factor**
Modifier les champs de commentaires	Quantification : **Modify Sample Comment**
Activer l'intégration manuelle	Quantification : **Manually integrate**
Définir le pic comme non trouvé	—
Inclure un pic dans le tableau de résultats ou l'en exclure	Quantification : **Exclude standards from calibration**
Options de régression	Quantification : **Change regression parameters**
Modifier les paramètres d'intégration du tableau de résultats pour un chromatogramme	Quantification : **Change "simple" parameters in peak review, Change "advanced" parameters in peak review**
Modifier la méthode de quantification du composant du tableau de résultats	Quantification : **Edit results tables' method**
Créer des paramètres de tracé métrique	Quantification : **Modify or create metric plot settings**
Ajouter des colonnes personnalisées	Quantification : **Create or modify formula columns**
Définir le format du titre de l'examen des pics	—
Supprimer la colonne personnalisée	Quantification : **Create or modify formula columns**

Tableau D-1 : Mappage des autorisations (suite)

Logiciel SCIEX OS	Logiciel Analyst
Paramètres d'affichage du tableau de résultats	Quantification : **Change results table column precision**, **Change results table column visibility**, **Modify results table settings**
Verrouiller le tableau de résultats	—
Déverrouiller le tableau de résultats	—
Marquer le fichier de résultats comme révisé et l'enregistrer	—
Modifier le modèle de rapport	Éditeur de modèle de rapport : **Create/ Modify report templates**
Transférer les résultats à LIMS	—
Modifier la colonne de code-barres	—
Modifier l'affectation d'échantillon de comparaison	—
Ajouter les spectres MSMS à la bibliothèque	Explorer : **Add spectrum to library record**
Paramètres par défaut du projet	Quantification : **Modify global (default) settings**
Créer un rapport dans tous les formats	—
Modifier les paramètres du critère de marquage	—
Modification du paramètre de suppression automatique des données aberrantes	—
Activer la suppression automatique des données aberrantes	—
Mettre à jour la méthode de traitement via FF/LS	—
Mettre à jour les résultats via FF/LS	—
Activer la fonction de regroupement par adduits	Quantification : **Create Analyte Groups**, **Modify Analyte Groups**
Rechercher des fichiers	—
Activer l'ajout de standards	—
Définir la règle de pourcentage d'intégration manuelle	Quantification : **Enable or Disable percent rule in Manual Integration**

Tableau D-1 : Mappage des autorisations (suite)

Logiciel SCIEX OS	Logiciel Analyst
Modifier le poids/volume	Quantification : **Modify Weight To Volume ratio**

Somme de contrôle du fichier de données E

Nous recommandons d'utiliser des sommes de contrôle de fichiers de données pour les fichiers wiff. La fonction de somme de contrôle est une vérification par redondance cyclique destinée à vérifier l'intégrité des fichiers de données.

Si la fonction Data File Checksum est activée, dès que l'utilisateur crée un fichier de données (wiff), le logiciel génère une valeur de somme de contrôle avec un algorithme reposant sur l'algorithme de chiffrement public MD5 et enregistre la valeur dans le fichier. Lorsque la somme de contrôle est vérifiée, le logiciel calcule la somme de contrôle et compare la somme de contrôle calculée à la somme de contrôle stockée dans le fichier.

La comparaison de la somme de contrôle peut donner trois résultats :

- Si les valeurs correspondent, la somme de contrôle est valide.
- Si les valeurs ne correspondent pas, la somme de contrôle n'est pas valide. Une somme de contrôle invalide indique soit que le fichier a été modifié en dehors du logiciel , soit que le fichier a été enregistré lorsque le calcul de la somme de contrôle était activé et que la somme de contrôle est différente de la somme de contrôle d'origine.
- Si le fichier ne contient aucune valeur de somme de contrôle, la somme de contrôle est introuvable. Un fichier ne contient pas de valeur de somme de contrôle, car le fichier a été enregistré lorsque la fonction Data File Checksum était désactivée.

Remarque : L'utilisateur peut vérifier la somme de contrôle à l'aide du logiciel Analyst. Consultez la documentation du logiciel Analyst.

Activer ou désactiver la fonction Data File Checksum

1. Ouvrez l'espace de travail Configuration.
2. Cliquez sur **Projets**.
3. Si nécessaire, développez **Sécurité du fichier de données**.
4. Pour activer la fonction de somme de contrôle du fichier de données, cochez la case **Activer l'écriture de la somme de contrôle pour la création de données wiff**. Pour désactiver cette fonction, décochez cette case.

Nous contacter

Formation destinée aux clients

- En Amérique du Nord : NA.CustomerTraining@sciex.com
- En Europe : Europe.CustomerTraining@sciex.com
- En dehors de l'UE et de l'Amérique du Nord, visitez le site sciex.com/education pour obtenir les coordonnées.

Centre d'apprentissage en ligne

- SCIEX Now Learning Hub

Assistance technique SCIEX

SCIEX et ses représentants disposent de personnel dûment qualifié et de spécialistes techniques dans le monde entier. Ils peuvent répondre aux questions sur le système ou tout problème technique qui pourrait survenir. Pour plus d'informations, consultez le site Web SCIEX à l'adresse sciex.com ou choisissez parmi les options suivantes pour nous contacter :

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

Cybersécurité

Pour obtenir les informations les plus récentes sur la cybersécurité des produits SCIEX, consultez la page sciex.com/productsecurity.

Documentation

Cette version du document remplace toutes les versions précédentes de ce document.

L'affichage électronique de ce document nécessite le lecteur Adobe Acrobat Reader. Pour télécharger la dernière version, accédez à https://get.adobe.com/reader.

Pour trouver la documentation du logiciel, consultez les notes de version ou le guide d'installation du logiciel fourni avec ce dernier.

La documentation du matériel se trouve dans la documentation fournie avec le système ou le composant.

Les dernières versions de la documentation sont disponibles sur le site Web SCIEX, à l'adresse sciex.com/customer-documents.

Nous contacter

Remarque : Pour demander une version imprimée gratuite de ce document, contactez sciex.com/contact-us.