
Logiciel SCIEX OS

Guide du directeur de laboratoire



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.

Les marques commerciales et/ou marques déposées mentionnées dans le présent document, y compris les logos associés, appartiennent à AB Sciex Pte. Ltd, ou à leurs propriétaires respectifs, aux États-Unis et/ou dans certains autres pays (voir sciex.com/trademarks).

AB Sciex™ est utilisé sous licence.

© 2022 DH Tech. Dev. Pte. Ltd.



AB Sciex Pte. Ltd.

B1k33, #04-06 Marsiling Industrial Estate Road 3

Woodlands Central Industrial Estate, Singapore 739256

Table des matières

Chapitre 1 : Introduction	6
Chapitre 2 : Présentation de la configuration de sécurité	7
Sécurité et conformité réglementaire	7
Exigences en matière de sécurité	7
SCIEX OS et sécurité Windows : une étroite collaboration	7
Registres d'audit dans SCIEX OS et Windows	8
Conseils de sécurité aux clients : sauvegardes	9
Norme 21 CFR Part 11	9
Configuration du système	10
Configuration de la sécurité Windows	10
Utilisateurs et groupes	10
Aide Active Directory	10
Système de fichiers Windows	11
Autorisations des fichiers et des dossiers	11
Audits du système	11
Registres d'événements	11
Alertes Windows	12
Chapitre 3 : Octroi d'une licence électronique	13
Emprunter une licence électronique sur serveur	13
Retourner une licence électronique sur serveur	14
Chapitre 4 : Contrôle d'accès à Analyst	16
Emplacement des informations de sécurité	16
Flux de travail de la sécurité logicielle	16
Installer SCIEX OS	17
Exigences du système	18
Options d'audit préreçlées	18
Configurer le Security Mode	18
Sélectionner le mode de sécurité	19
Configurer les options de sécurité du poste de travail (Mixed Mode)	19
Configurer une notification par e-mail (Mixed Mode)	20
Configurez l'accès à SCIEX OS	21
Autorisations SCIEX OS	22
À propos des utilisateurs et des rôles	31
Gérer les utilisateurs	42
Gérer les rôles	43
Exporter et importer les paramètres de gestion des utilisateurs	44
Exporter les paramètres de gestion des utilisateurs	44
Importer les paramètres de gestion des utilisateurs	45

Table des matières

Restaurer les paramètres de gestion des utilisateurs	45
Configurer l'accès aux projets et aux fichiers de projets	45
Dossiers du projet	46
Types de fichier du logiciel	46
Chapitre 5 : Central Administrator Console	49
Utilisateurs	49
Groupe d'utilisateurs	49
Rôles utilisateur et autorisations	50
Groupes de travail	62
Créer un groupe de travail	62
Supprimer un groupe de travail	62
Ajouter des utilisateurs ou des groupes à un groupe de travail	63
Ajouter des postes de travail à un groupe de travail	64
Ajouter des projets à un groupe de travail	64
Gérer des projets	65
À propos des projets et des répertoires racines	65
Ajouter un répertoire racine	66
Supprimer un répertoire racine de projet	66
Ajouter un projet	67
Ajouter un sous-dossier	67
Postes de travail	68
Ajouter un poste de travail	68
Supprimer un poste de travail	68
Rapports et fonctions de sécurité	68
Générer des rapports de données de groupe de travail	68
Exporter les paramètres du logiciel de CAC	69
Importer les paramètres du logiciel de CAC	69
Restaurer les paramètres logiciels CAC	70
Chapitre 6 : Acquisition réseau	71
À propos de l'acquisition réseau	71
Avantages de l'utilisation de l'acquisition réseau	71
Compte réseau sécurisé	72
Processus de transfert de données	72
Configurer l'acquisition réseau	72
Spécifier un compte réseau sécurisé	73
Chapitre 7 : Audit	74
Registres d'audit	74
Cartes d'audit	75
Configuration des cartes d'audit	76
Modèles de carte d'audit installés	76
Travailler avec des cartes d'audit	77
Cartes d'audit de projet	77
Cartes d'audit de poste de travail	79
Afficher, rechercher, exporter et imprimer des registres d'audit	81
Afficher un registre d'audit	81

Rechercher ou filtrer des enregistrements d'audit.....	82
Afficher un registre d'audit archivé.....	82
Imprimer un registre d'audit.....	82
Exporter les enregistrements du registre d'audit.....	82
Enregistrements dans le registre d'audit.....	83
Archives de registres d'audit.....	83
Annexe A : Accéder aux données pendant des interruptions du réseau.....	85
Afficher et traiter des données localement.....	85
Retirer des échantillons des dossiers de transfert réseau.....	85
Annexe B : Événements d'audit.....	87
Annexe C : Mappage d'autorisations entre SCIEX OS et le logiciel Analyst.....	94
Annexe D : Somme de contrôle du fichier de données.....	100
Activer ou désactiver la fonction Data File Checksum.....	100
Nous contacter.....	101
Formation destinée aux clients.....	101
Centre d'apprentissage en ligne.....	101
Assistance technique SCIEX.....	101
Cybersécurité.....	101
Documentation.....	101

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

- 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 de SCIEX OS fonctionnent conjointement avec les composants d'audit et de contrôle d'accès de Windows. En outre, elle décrit comment configurer la sécurité Windows avant l'installation de SCIEX OS.

Sécurité et conformité réglementaire

SCIEX OS offre :

- 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.

SCIEX OS et sécurité Windows : une étroite collaboration

SCIEX OS et le système 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](#).

SCIEX OS comporte 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 Security Mode](#).

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 [Configurez l'accès à SCIEX OS](#).

Registres d'audit dans SCIEX OS et Windows

Les fonctions d'audit dans SCIEX OS ainsi que les composants d'audit intégrés à Windows sont essentiels à la création et à la gestion des 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 des rôles et la suppression des 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.

Remarque : SCIEX OS n'audit pas la création ni les modifications apportées aux méthodes MS, aux méthodes LC, aux lots ni aux méthodes de traitement. Ces fichiers servent de modèles. Les valeurs des paramètres y sont lues au moment de l'acquisition ou du traitement et appliqués à la tâche. Pour les méthodes MS, les méthodes LC et les lots, les valeurs des paramètres sont enregistrées dans les fichiers wiff et wiff2. Les méthodes de traitement sont enregistrées dans le fichier qsession. Ces fichiers servent d'enregistrements électroniques pour ces informations.

Pour obtenir une liste complète des événements d'audit, consultez la section [Événements d'audit](#).

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 la faible éventualité où un correctif de sécurité affecterait le fonctionnement d'une application.

Norme 21 CFR Part 11

SCIEX OS contient les contrôles techniques pour prendre en charge 21 CFR Part 11 avec l'implémentation 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.

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 se conformer à cette dernière. La conformité de l'utilisation de SCIEX OS à la norme 21 CFR Part 11 dépend de l'usage et de la configuration réels de SCIEX OS au sein du laboratoire.

Des services de validation sont disponibles grâce aux services professionnels de SCIEX. Pour plus d'informations, contactez complianceservices@sciex.com.

Remarque : Ne laissez pas le logiciel Instrument Parameters Converter sur un système validé. Il est prévu pour le transfert initial des paramètres de l'instrument du logiciel Analyst vers SCIEX OS. Veillez à retirer le logiciel Instrument Parameters 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

Le système implémente les restrictions suivantes pour les comptes utilisateurs locaux 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**, **administrator** ni **demo**.

L'administrateur de SCIEX OS doit avoir la possibilité de modifier les autorisations de fichiers pour le dossier de données SCIEX OS. 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 disposent de l'accès requis aux ressources en vue de l'acquisition réseau, l'administrateur réseau peut définir 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.

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, se reporter à la section : [Configurez l'accès à SCIEX OS](#).

Aide Active Directory

Lors de l'ajout d'utilisateurs dans l'espace de travail Configuration de SCIEX OS, spécifiez les comptes d'utilisateurs au format User Principal Name (UPN). 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 SCIEX OS, les fichiers et les répertoires doivent être stockés sur une partition de disque dur qui utilise le format NTFS, qui peut contrôler et auditer l'accès aux fichiers SCIEX OS. Le système de fichier FAT (table d'allocation de fichiers) 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 de 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, reportez-vous à la documentation Windows.

Pour obtenir des informations sur les autorisations de fichiers et de dossiers de 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, reportez-vous à 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 SCIEX OS, les licences électroniques peuvent être des licences avec blocage de nœud ou des licences sur serveur. Pour le logiciel Central Administrator Console (CAC), les licences électroniques ne peuvent être que des licences avec blocage de nœud.

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 **Licenses** dans la fenêtre SCIEX OS.

Remarque : Veillez à bien renouveler la licence avant qu'elle n'arrive à expiration.

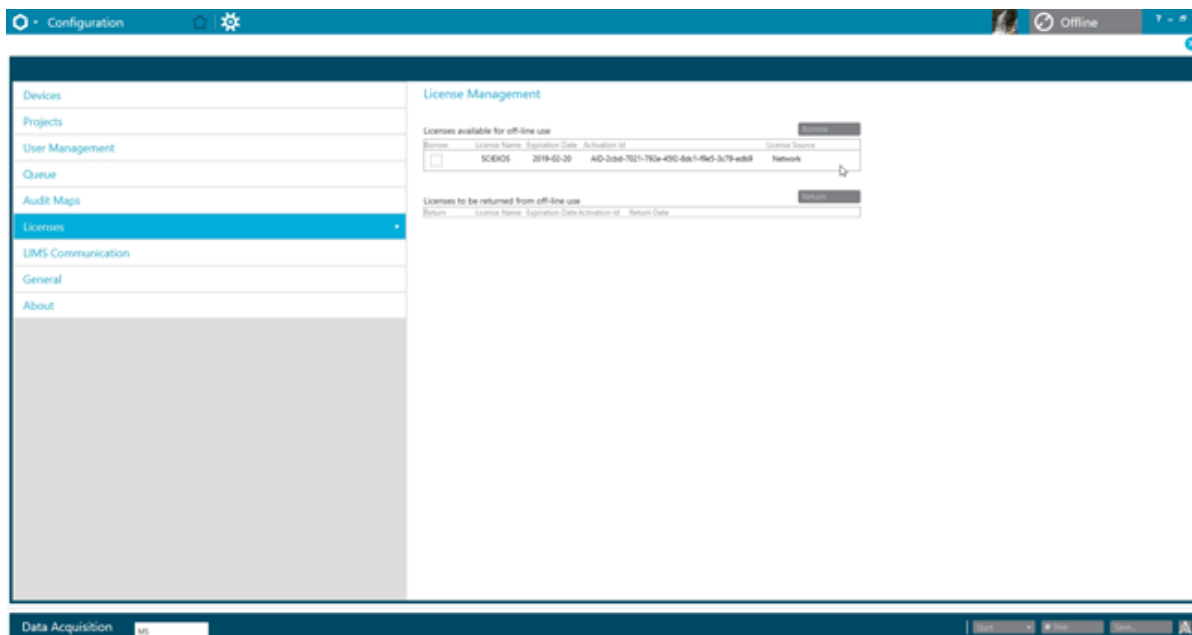
Emprunter une licence électronique sur serveur

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 **Licenses**.
Le tableau Licenses available for off-line use affiche toutes les licences disponibles à l'emprunt.

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



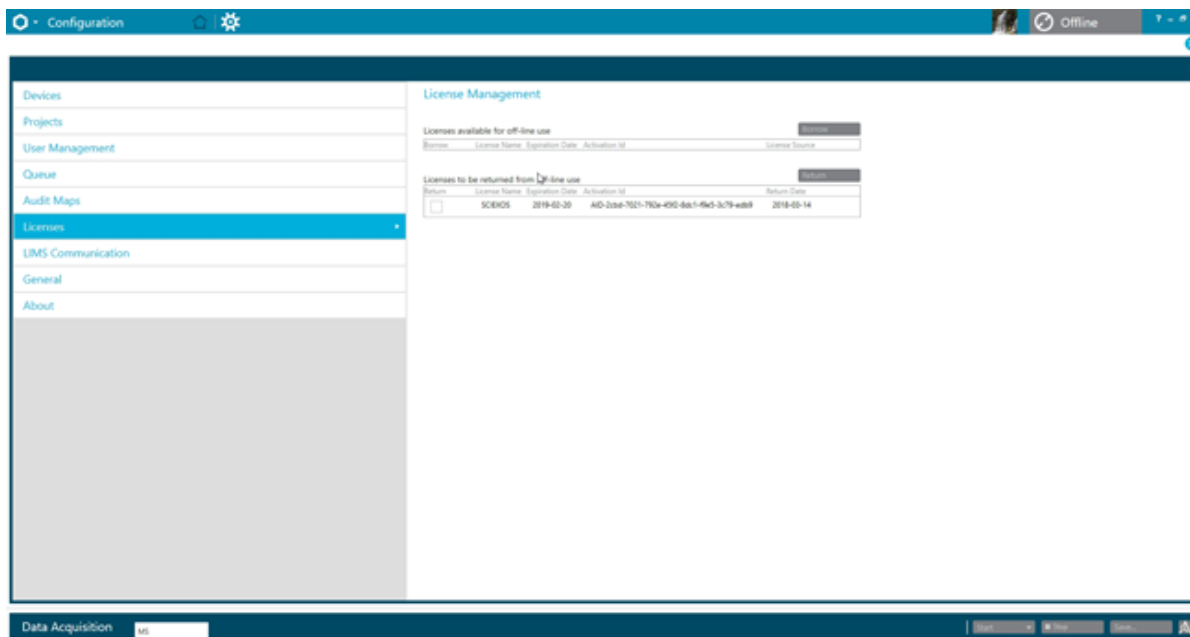
3. Sélectionnez la licence à emprunter, puis cliquez sur **Borrow**.

Retourner 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 **Licenses**.
Le tableau Licenses to be returned from off-line use présente toutes les licences qui peuvent être retournées (toutes les licences empruntées par cet ordinateur).

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



3. Sélectionnez la licence à retourner, puis cliquez sur **Return**.

Cette section décrit comment contrôler l'accès à SCIEX OS. Pour contrôler l'accès à SCIEX OS, 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 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 présente des instructions pour l'administration locale de SCIEX OS. Pour l'administration centralisée de SCIEX OS, voir 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

SCIEX OS fonctionne 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 SCIEX OS : capacité à ouvrir SCIEX OS.
- Autorisation 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 SCIEX OS.	Consulter le document : <i>Guide d'installation du logiciel SCIEX OS</i> .
Configurer l'accès à SCIEX OS.	Consulter la section Configurez l'accès à SCIEX OS
Configurer Windows File Security et NTFS.	Consulter la section Configurer l'accès aux projets et aux fichiers de projets .

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 de SCIEX OS	
Installer 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 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 SCIEX OS

Avant d'installer 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 et à réaliser la séquence d'installation qui convient.

Exigences du système

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

Options d'audit préréglées

Pour obtenir une description des cartes d'audit installées, se reporter à la section : [Modèles de carte d'audit installés](#). Après l'installation, l'administrateur de SCIEX OS peut créer des cartes d'audit personnalisées et attribuer une autre carte d'audit dans l'espace de travail Configuration.

Configurer le Security Mode

Cette section décrit les options Security Mode sur la page User Management dans l'espace de travail Configuration.

Integrated Mode : si l'utilisateur actuellement connecté à Windows est défini comme un utilisateur dans le logiciel, cet utilisateur a accès à SCIEX OS.

Integrated Mode : si l'utilisateur actuellement connecté à Windows est défini comme un utilisateur dans le logiciel, cet utilisateur a accès au logiciel .

Mixed Mode : les utilisateurs se connectent séparément à Windows et au logiciel. Il n'est pas nécessaire que les identifiants de connexion à Windows et à 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 Integrated.

Si le mode Mixed est sélectionné, les fonctionnalités Screen Lock et Auto Logoff sont prêtes à être utilisées.

Screen Lock et Auto Logoff : 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 Screen Lock et Auto Logoff sont disponibles en mode Mixed 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 Results Table 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.

Security Notification : 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 **User Management**.
3. Cliquez sur l'onglet **Security Mode**.
4. Sélectionnez **Integrated Mode** ou **Mixed Mode**. Consulter la section : [Configurer le Security Mode](#)
5. Cliquez sur **Save**.
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. Consulter la section : [Configurer le Security Mode](#)

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 **User Management**.
3. Ouvrez l'onglet Security Mode.
4. Respectez les étapes suivantes pour configurer la fonction Screen Lock :
 - a. Sélectionnez **Screen Lock**.
 - b. Dans le champ **Wait**, 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 **Auto Logoff**.
 - b. Dans le champ **Wait**, 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 **Save**.

Contrôle d'accès à Analyst

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. Consulter la section : [Configurer le Security Mode](#)

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 **User Management**.
3. Ouvrez l'onglet Security Mode.
4. Cochez la case **Send e-mail messages after** 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 **Send e-mail messages after**.

5. Dans le champ **SMTP Server**, 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 **Port Number**, inscrivez le numéro du port ouvert.
Cliquez sur **Apply Default** pour insérer le numéro de port par défaut, 25.
7. Dans le champ **To**, saisissez l'adresse électronique à laquelle le message doit être envoyé. Par exemple : username@domain.com.
8. Dans le champ **From**, saisissez l'adresse électronique à afficher dans le champ **From** du message.
9. Dans le champ **Subject**, inscrivez le sujet du message.
10. Dans le champ **Message**, saisissez le texte à inclure dans le corps du message.
11. Cliquez sur **Save**.
Une boîte de dialogue de confirmation apparaît.
12. Cliquez sur **OK**.
13. Pour vérifier la configuration, cliquez sur **Send Test Mail**.

Configurez l'accès à 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. Parlez des politiques de groupe avec l'administrateur Active Directory dans le cadre d'un déploiement global de SCIEX OS.

Autorisations SCIEX OS

Illustration 4-1 : Page User Management

Permission	Administrator	Method Developer	Analyst	Reviewer
Batch				
Submit unlocked methods	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Open	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Save as	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Submit	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Save	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Save ion reference table	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Add data sub-folders	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Configure Decision Rules	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Configuration				
General tab	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
General: change regional setting	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
General: full screen mode	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LIMS communication tab	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Tableau 4-3 : Autorisations

Autorisation	Description
Batch (Lot)	
Submit unlocked methods	(Soumettre les méthodes déverrouillées) Permet aux utilisateurs de soumettre des lots contenant des méthodes déverrouillées.
Open	(Ouvrir) Permet aux utilisateurs d'ouvrir des lots existants.
Save as	(Enregistrer sous) Permet aux utilisateurs d'enregistrer des lots sous un nouveau nom.
Submit	(Soumettre) Permet aux utilisateurs de soumettre des lots.
Save	(Enregistrer) Permet aux utilisateurs d'enregistrer un lot en écrasant le contenu existant.

Tableau 4-3 : Autorisations (suite)

Autorisation	Description
Save ion reference table	(Enregistrer le tableau de référence d'ions) Permet aux utilisateurs d'éditer le tableau de référence d'ions.
Add data sub-folders	(Ajouter des sous-dossiers de données) Permet aux utilisateurs de créer des sous-dossiers pour stocker des données.
Configure Decision Rules	(Configurer des règles de décision) Permet aux utilisateurs d'ajouter et de modifier des règles de décision.
Configuration (Configuration)	
General tab	(Onglet Général) Permet aux utilisateurs d'ouvrir la page General dans l'espace de travail Configuration.
General: change regional setting	(Général : modifier le paramètre régional) Permet aux utilisateurs d'appliquer les paramètres régionaux actuels du système à SCIEX OS.
General: full screen mode	(Général : mode plein écran) Permet aux utilisateurs d'activer et de désactiver le mode plein écran.
General: Stop Windows services	(Général : arrêter les services Windows) Permet aux utilisateurs d'activer ou désactiver l'option Windows Settings .
LIMS communication tab	(Onglet Communication LIMS) Permet aux utilisateurs d'ouvrir la page LIMS Communication dans l'espace de travail Configuration.
Audit maps tab	(Onglet Cartes d'audit) Permet aux utilisateurs d'ouvrir la page Audit Maps dans l'espace de travail Configuration.
Queue tab	(Onglet File d'attente) Permet aux utilisateurs d'ouvrir la page Queue dans l'espace de travail Configuration.
Queue: instrument idle time	(File d'attente : période d'inactivité de l'instrument) Permet aux utilisateurs de définir la période d'inactivité de l'instrument.
Queue: max number of acquired samples	(File d'attente : nombre maxi d'échantillons acquis) Permet aux utilisateurs de définir le nombre maximum autorisé d'échantillons acquis.
Queue: other queue settings	(File d'attente : autres paramètres de file d'attente) Permet aux utilisateurs de configurer d'autres paramètres de file d'attente.
Projects tab	(Onglet Projets) Permet aux utilisateurs d'ouvrir la page Projects dans l'espace de travail Configuration.

Contrôle d'accès à Analyst

Tableau 4-3 : Autorisations (suite)

Autorisation	Description
Projects: create project	(Projets : créer projet) Permet aux utilisateurs de créer des projets.
Projects: apply an audit map template to an existing project	(Projets : appliquer un modèle de carte d'audit à un projet existant) Permet aux utilisateurs d'appliquer une carte d'audit à un projet.
Projects: create root directory	(Projets : créer un répertoire racine) Permet aux utilisateurs de créer un répertoire racine pour stocker des projets.
Projects: set current root directory	(Projets : définir le répertoire racine actuel) Permet aux utilisateurs de modifier le répertoire racine pour un projet.
Projects: specify network credentials	(Projets : spécifier les identifiants du réseau) Permet aux utilisateurs de spécifier un compte réseau sécurisé (SNA) à utiliser pendant l'acquisition réseau si l'utilisateur connecté n'a pas accès à la ressource réseau.
Projects: Enable checksum writing for wiff data creation	(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 pour les fichiers de données wiff.
Projects: clear root directory	(Projets : effacer un répertoire racine) Permet aux utilisateurs de supprimer un répertoire racine de la liste.
Devices tab	(Onglet Appareils) Permet aux utilisateurs d'ouvrir la page Devices dans l'espace de travail Configuration.
User management tab	(Onglet Gestion des utilisateurs) Permet aux utilisateurs d'ouvrir la page User Management dans l'espace de travail Configuration.
Force user logoff	(Forcer la déconnexion de l'utilisateur) Permet aux utilisateurs de forcer la déconnexion d'un utilisateur actuellement connecté à SCIEX OS. Permet aux utilisateurs de forcer la déconnexion d'un utilisateur actuellement connecté au logiciel SCIEX OS.
Event Log (Registre des événements)	
Access event log workspace	(Accéder à l'espace de travail du registre des événements) Permet aux utilisateurs d'ouvrir l'espace de travail Event Log.
Archive log	(Registre d'archive) Permet aux utilisateurs d'archiver le journal des événements.
Audit Trail (Registre d'audit)	
Access audit trail workspace	(Accéder à l'espace de travail du registre d'audit) Permet aux utilisateurs d'ouvrir l'espace de travail Audit Trail.

Tableau 4-3 : Autorisations (suite)

Autorisation	Description
View active audit map	(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 Registre d'audit.
Print/Export audit trail	(Imprimer/Exporter le registre d'audit) Permet aux utilisateurs d'imprimer ou exporter le registre d'audit.
CAC Server (Serveur CAC) (CAC uniquement)	
Manage Workgroups	(Gérer les groupes de travail) Permet aux utilisateurs de créer et gérer des groupes de travail dans l'espace de travail User Management.
Manage Workgroups Projects	(Gérer les projets de groupes de travail) Permet aux utilisateurs de créer et gérer des projets de groupes de travail dans l'espace de travail User Management.
Data Acquisition Panel (Volet Data Acquisition)	
Start	(Commencer) Permet aux utilisateurs de commencer l'acquisition dans le volet Data Acquisition.
Stop	(Arrêter) Permet aux utilisateurs d'arrêter l'acquisition dans le volet Data Acquisition.
Save	(Enregistrer) Permet aux utilisateurs d'enregistrer les données acquises sous un autre nom de fichier dans le volet Data Acquisition.
MS & LC Method (Méthodes MS et LC)	
Access method workspace	(Accéder à l'espace de travail de méthode) Permet aux utilisateurs d'ouvrir les espaces de travail MS Method et LC Method.
New	(Nouveau) Permet aux utilisateurs de créer des méthodes MS et LC.
Open	(Ouvrir) Permet aux utilisateurs d'ouvrir des méthodes MS et LC.
Save	(Enregistrer) Permet aux utilisateurs d'enregistrer une méthode en écrasant le contenu existant.
Save as	(Enregistrer sous) Permet aux utilisateurs d'enregistrer des méthodes sous un nouveau nom.
Lock/Unlock method	(Verrouiller/Déverrouiller la méthode) Permet aux utilisateurs de verrouiller les méthodes pour empêcher toute modification et de les déverrouiller.
Queue (File d'attente)	

Contrôle d'accès à Analyst

Tableau 4-3 : Autorisations (suite)

Autorisation	Description
Manage	(Gérer) Permet aux utilisateurs d'ouvrir l'espace de travail Queue.
Start/Stop	(Commencer/Arrêter) Permet aux utilisateurs de commencer ou d'arrêter la file d'attente.
Print	(Imprimer) Permet aux utilisateurs d'imprimer la file d'attente.
Library (Bibliothèque)	
Access library workspace	(Accéder à l'espace de travail Bibliothèque) Permet aux utilisateurs d'ouvrir l'espace de travail Library. Pas applicable au flux de travail Quantitation.
CAC settings (Client CAC)	
Enable Central Administration	(Activer Central Administration) Permet aux utilisateurs de configurer SCIEX OS pour l'administration centrale avec le logiciel Central Administrator Console (CAC).
MS Tune (Réglage MS)	
Access MS Tune workspace	(Accéder à l'espace de travail Réglage MS) Permet aux utilisateurs d'ouvrir l'espace de travail MS Tune.
Advanced MS tuning	(Réglage MS avancé) (Systèmes X500 QTOF) Permet aux utilisateurs d'accéder aux options d'ajustement avancées, notamment Detector Optimization, Positive and Negative Q1 Unit Tuning, Positive and Negative TOF MS Tuning et Positive and Negative Q1 High Tuning.
Advanced troubleshooting	(Dépannage avancé) Permet aux utilisateurs d'ouvrir la boîte de dialogue Advanced Troubleshooting.
Quick status check	(Contrôle d'état rapide) (Systèmes X500 QTOF) Permet aux utilisateurs d'effectuer les contrôles d'état rapides positifs et négatifs.
Restore instrument data	(Restaurer les données de l'instrument) Permet aux utilisateurs de restaurer les paramètres de réglage enregistrés auparavant.
Explorer (Explorer)	
Access Explorer workspace	(Accéder à l'espace de travail Explorer) Permet aux utilisateurs d'ouvrir l'espace de travail Explorer.
Export	(Exporter) Permet aux utilisateurs d'exporter des données depuis l'espace de travail Explorer.
Print	(Imprimer) Permet aux utilisateurs d'imprimer des données dans l'espace de travail Explorer.

Tableau 4-3 : Autorisations (suite)

Autorisation	Description
Options	(Options) Permet aux utilisateurs de modifier les options de l'espace de travail Explorer.
Recalibrate	(Réétalonner) Permet aux utilisateurs de réétalonner les échantillons et les spectres dans l'espace de travail Explorer. Pas applicable au flux de travail Quantitation.
Analytics (Analytique)	
New results	(Nouveaux résultats) Permet aux utilisateurs de créer des tableaux de résultats.
Create processing method	(Créer une méthode de traitement) Permet aux utilisateurs de créer des méthodes de traitement.
Modify processing method	(Modifier une méthode de traitement) Permet aux utilisateurs de modifier des méthodes de traitement.
Allow Export and Create Report of unlocked Results Table	(Autoriser l'exportation et la création d'un rapport du tableau de résultats déverrouillé) Permet aux utilisateurs d'exporter ou de générer un rapport depuis un Results Table ou un tableau de statistiques, si le Results Table n'est pas verrouillé.
Save results for Automation Batch	(Sauvegarder les résultats pour le lot d'automatisation) Permet de sauvegarder les tableaux de résultats créés automatiquement dans l'espace de travail Batch. Cette autorisation est requise pour le traitement automatique pendant l'acquisition.
Change default quantitation method integration algorithm	(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.
Change default quantitation method integration parameters	(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.
Enable project modified peak warning	(Activer l'avertissement de pic modifié du projet) Permet aux utilisateurs d'activer la propriété d'avertissement de pic modifié pour un projet.
Add samples	(Ajouter des échantillons) Permet aux utilisateurs d'ajouter des échantillons à un tableau de résultats.
Remove selected samples	(Retirer les échantillons sélectionnés) Permet aux utilisateurs de retirer les échantillons sélectionnés d'un tableau de résultats.

Tableau 4-3 : Autorisations (suite)

Autorisation	Description
Export, import, or remove external calibration	(Exporter, importer ou supprimer un étalonnage externe) Permet aux utilisateurs d'exporter, importer ou supprimer des étalonnages externes.
Modify sample name	(Modifier le nom de l'échantillon) Permet aux utilisateurs de modifier le nom de l'échantillon dans le tableau de résultats.
Modify sample type	(Modifier le type d'échantillon) Permet aux utilisateurs de modifier le type d'échantillon, tel que standard, contrôle qualité (CQ) ou inconnu, dans le tableau de résultats.
Modify sample ID	(Modifier l'ID de l'échantillon) Permet aux utilisateurs de modifier l'ID de l'échantillon dans le tableau de résultats.
Modify actual concentration	(Modifier la concentration réelle) Permet aux utilisateurs de modifier la concentration réelle des échantillons standard et de contrôle qualité dans le tableau de résultats.
Modify dilution factor	(Modifier le facteur de dilution) Permet aux utilisateurs de modifier le facteur de dilution dans le tableau de résultats.
Modify comment fields	(Modifier les champs de commentaires) Permet aux utilisateurs de modifier les champs de commentaires : <ul style="list-style-type: none"> • Component Comment • IS Comment • IS Peak Comment • Peak Comment • Sample Comment
Enable manual integration	(Activer l'intégration manuelle) Permet aux utilisateurs de procéder à l'intégration manuelle.
Set peak to Not Found	(Définir le pic sur Introuvable) Permet aux utilisateurs de définir un pic sur Not Found .
Include or exclude a peak from the Results Table	(Inclure un pic au tableau de résultats ou l'en exclure) Permet aux utilisateurs d'inclure un pic au tableau de résultats ou de l'en exclure.
Regression options	(Options de régression) Permet aux utilisateurs de modifier les options de régression dans le volet Calibration Curve.
Modify Results Table integration parameters for a single chromatogram	(Modifier les paramètres d'intégration des tableaux de résultats pour un chromatogramme unique) Permet aux utilisateurs de modifier les paramètres d'intégration pour un chromatogramme unique dans le volet Examen de pic.

Tableau 4-3 : Autorisations (suite)

Autorisation	Description
Modify quantitation method for the Results Table component	(Modifier la méthode de quantification pour le composant Tableau de résultats) Permet aux utilisateurs de sélectionner une méthode de traitement différente pour un composant dans le volet Examen de pic avec l'option Update Processing Method for Component .
Create metric plot new settings	(Créer de nouveaux paramètres de graphique métrique) Permet aux utilisateurs de créer de nouveaux graphiques métriques et de modifier les réglages.
Add custom columns	(Ajouter des colonnes personnalisées) Permet aux utilisateurs d'ajouter des colonnes personnalisées à un tableau de résultats.
Set peak review title format	(Définir le format du titre de l'examen de pic) Permet aux utilisateurs de modifier le titre de l'examen de pic.
Remove custom column	(Supprimer la colonne personnalisée) Permet aux utilisateurs de supprimer des colonnes personnalisées d'un tableau de résultats.
Results Table display settings	(Paramètres d'affichage du tableau de résultats) Permet aux utilisateurs de personnaliser les colonnes dans le tableau de résultats.
Lock Results Table	(Verrouiller le tableau de résultats) Permet aux utilisateurs de verrouiller un tableau de résultats pour éviter toute modification.
Unlock Results Table	(Déverrouiller le tableau de résultats) Permet aux utilisateurs de déverrouiller un tableau de résultats pour permettre des modifications.
Mark Results file as reviewed and save	(Marquer le fichier de résultats comme révisé et l'enregistrer) Permet aux utilisateurs de marquer un tableau de résultats comme révisé et de l'enregistrer.
Modify report template	(Modifier le modèle de rapport) Permet aux utilisateurs de modifier les modèles de rapports.
Transfer results to LIMS	(Transférer les résultats vers LIMS) Permet aux utilisateurs de charger les résultats dans un système de gestion des informations de laboratoire (LIMS).
Modify barcode column	(Modifier la colonne de code-barres) Permet aux utilisateurs de supprimer la colonne Barcode dans un tableau de résultats.

Tableau 4-3 : Autorisations (suite)

Autorisation	Description
Change comparison sample assignment	(Modifier l'affectation de l'échantillon de comparaison) Permet aux utilisateurs de modifier l'échantillon de comparaison spécifié dans la colonne Comparison du tableau de résultats.
Add the MSMS spectra to library	(Ajouter les spectres MSMS à la bibliothèque) Permet aux utilisateurs d'ajouter les spectres MS/MS sélectionnés à une bibliothèque. Pas applicable au flux de travail Quantitation.
Project default settings	(Paramètres par défaut du projet) Permet aux utilisateurs de modifier les paramètres de traitement quantitatif et qualitatif par défaut du projet.
Create report in all formats	(Créer un rapport sous tous les formats) Permet aux utilisateurs de générer des rapports sous tous les formats. Les utilisateurs sans cette autorisation peuvent uniquement générer des rapports au format PDF.
Edit flagging criteria parameters	(Modifier les paramètres des critères de marquage) Permet aux utilisateurs de modifier les paramètres de marquage dans une méthode de traitement.
Automatic outlier removal parameter change	(Modifier les paramètres de suppression automatique des données aberrantes) Permet aux utilisateurs de modifier les paramètres pour la suppression automatique des données aberrantes.
Enable automatic outlier removal	(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.
Update processing method via FF/LS	(Mettre à jour la méthode de traitement via FF/LS) Permet aux utilisateurs de mettre à jour les méthodes de traitement à l'aide de Formula Finder et de Library Search. Pas applicable au flux de travail Quantitation.
Update results via FF/LS	(Mettre à jour les résultats via FF/LS) Permet aux utilisateurs de mettre à jour les résultats à l'aide de Formula Finder et de Library Search. Pas applicable au flux de travail Quantitation.
Enable grouping by adducts functionality	(Activer la fonction de regroupement par adduits) Permet aux utilisateurs de mettre à jour la méthode de traitement pour activer la fonction de regroupement d'adduits.
Browse for files	(Naviguer vers les fichiers) Permet aux utilisateurs de naviguer hors du dossier de données local.

Tableau 4-3 : Autorisations (suite)

Autorisation	Description
Enable standard addition	(Activer l'ajout standard) Permet aux utilisateurs de mettre à jour la méthode de traitement pour activer la fonction d'ajout de standard.
Set Manual Integration Percentage Rule	(Définir la règle de pourcentage d'intégration manuelle) Permet aux utilisateurs de modifier le paramètre Manual Integration % .

À propos des utilisateurs et des rôles

Dans SCIEX OS, l'administrateur peut ajouter des utilisateurs et groupes Windows à la base de données de gestion des utilisateurs pour SCIEX OS. 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.

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 rôles déterminent les fonctions accessibles à l'utilisateur. Les rôles prédéfinis ne peuvent pas être supprimés et leurs autorisations ne peuvent pas être modifiées.

Remarque : Pour les groupes de travail administrés par le logiciel Central Administrator Console (CAC), les pages User Management sont en lecture seule.

Tableau 4-4 : Rôles prédéfinis

Rôle	Tâches habituelles
Administrator (Administrateur)	<ul style="list-style-type: none"> Gère le système. Configure la sécurité.
Method Developer (Développeur de méthode)	<ul style="list-style-type: none"> Crée des méthodes. Exécute des lots. Analyse les données à utiliser par l'utilisateur final.
Analyst (Analyst)	<ul style="list-style-type: none"> Exécute des lots. Analyse les données à utiliser par l'utilisateur final.
Reviewer (Réviseur)	<ul style="list-style-type: none"> Examine les données. Examine les registres d'audit. Examine les résultats de quantification.

Contrôle d'accès à Analyst

Tableau 4-5 : Autorisations prédéfinies

Autorisation	Administrateur	Développeur de méthode	Analyst	Examineur
Batch (Lot)				
Submit unlocked methods (Soumettre les méthodes déverrouillées)	✓	✓	✓	×
Open (Ouvrir)	✓	✓	✓	✓
Save as (Enregistrer sous)	✓	✓	✓	×
Submit (Envoyer)	✓	✓	✓	×
Save (Enregistrer)	✓	✓	✓	×
Save ion reference table (Enregistrer le tableau de référence d'ions)	✓	✓	✓	×
Add data sub-folders (Ajouter des sous-dossiers de données)	✓	✓	✓	×
Configure Decision Rules (Configurer les règles de décision)	✓	✓	✓	×
Configuration (Configuration)				
General tab (Onglet General)	✓	✓	×	×
General: change regional setting (Général : modifier le paramètre régional)	✓	✓	×	×
General: full screen mode (Général : mode plein écran)	✓	✓	×	×
General: Stop Windows services (Général : arrêter les services Windows)	✓	×	×	×
LIMS communication tab (Onglet Communication LIMS)	✓	✓	×	×

Tableau 4-5 : Autorisations prédéfinies (suite)

Autorisation	Administrateur	Développeur de méthode	Analyst	Examineur
Audit maps tab (Onglet Cartes d'audit)	✓	×	×	×
Queue tab (Onglet File d'attente)	✓	✓	✓	✓
Queue: instrument idle time (File d'attente : période d'inactivité de l'instrument)	✓	✓	×	×
Queue: max number of acquired samples (File d'attente : nombre max. d'échantillons acquis)	✓	✓	×	×
Queue: other queue settings (File d'attente : autres paramètres de file d'attente)	✓	✓	×	×
Projects tab (Onglet Projets)	✓	✓	✓	✓
Projects: create project (Projets : créer projet)	✓	✓	✓	×
Projects: apply an audit map template to an existing project (Projets : appliquer un modèle de carte d'audit à un projet existant)	✓	×	×	×
Projects: create root directory (Projets : créer un répertoire racine)	✓	×	×	×
Projects: set current root directory (Projets : définir le répertoire racine actuel)	✓	×	×	×

Contrôle d'accès à Analyst

Tableau 4-5 : Autorisations prédéfinies (suite)

Autorisation	Administrateur	Développeur de méthode	Analyst	Examineur
Projects: specify network credentials (Projets : spécifier les identifiants du réseau)	✓	x	x	x
Projects: Enable checksum writing for wiff1 data creation (Projets : activer l'écriture de somme de contrôle pour la création de données wiff1)	✓	x	x	x
Projects: clear root directory (Projets : effacer un répertoire racine)	✓	x	x	x
Devices tab (Onglet Appareils)	✓	✓	✓	x
User management tab (Onglet Gestion des utilisateurs)	✓	x	x	x
Force user logoff (Forcer la déconnexion des utilisateurs)	✓	x	x	x
Event Log (Registre des événements)				
Access event log workspace (Accéder à l'espace de travail du registre des événements)	✓	✓	✓	✓
Archive log (Registre d'archive)	✓	✓	✓	✓
Audit Trail (Registre d'audit)				
Access audit trail workspace (Accéder à l'espace de travail du registre d'audit)	✓	✓	✓	✓

Tableau 4-5 : Autorisations prédéfinies (suite)

Autorisation	Administrateur	Développeur de méthode	Analyst	Examineur
View active audit map (Afficher la carte d'audit active)	✓	✓	✓	✓
Print/Export audit trail (Imprimer/ Exporter le registre d'audit)	✓	✓	✓	✓
Data Acquisition Panel (Volet Data Acquisition)				
Start (Démarrer)	✓	✓	✓	×
Stop (Arrêter)	✓	✓	✓	×
Save (Enregistrer)	✓	✓	✓	×
MS & LC Method (Méthodes MS et LC)				
Access method workspace (Accéder à l'espace de travail de méthode)	✓	✓	✓	✓
New (Nouveau)	✓	✓	×	×
Open (Ouvrir)	✓	✓	✓	✓
Save (Enregistrer)	✓	✓	×	×
Save as (Enregistrer sous)	✓	✓	×	×
Lock/Unlock method (Verrouiller/ Déverrouiller la méthode)	✓	✓	×	×
Queue (File d'attente)				
Manage (Gestion)	✓	✓	✓	×
Start/Stop (Démarrer/ Arrêter)	✓	✓	✓	×
Print (Imprimer)	✓	✓	✓	✓
Library (Bibliothèque)				

Contrôle d'accès à Analyst

Tableau 4-5 : Autorisations prédéfinies (suite)

Autorisation	Administrateur	Développeur de méthode	Analyst	Examineur
Access library workspace (Accéder à l'espace de travail Bibliothèque)	✓	✓	✓	✓
CAC settings (Client CAC)				
Enable Central Administration (Activer Central Administration)	✓	x	x	x
MS Tune (Réglage MS)				
Access MS Tune workspace (Accéder à l'espace de travail Réglage MS)	✓	✓	✓	x
Advanced MS Tuning (Réglage MS avancé)	✓	✓	x	x
Advanced troubleshooting (Dépannage avancé)	✓	✓	x	x
Quick status check (Contrôle d'état rapide)	✓	✓	✓	x
Restore instrument data (Restaurer les données de l'instrument)	✓	✓	x	x
Explorer (Explorer)				
Access explorer workspace (Accéder à l'espace de travail Explorer)	✓	✓	✓	✓
Export (Exporter)	✓	✓	✓	x
Print (Imprimer)	✓	✓	✓	x
Options (Options)	✓	✓	✓	x
Recalibrate (Réétalonner)	✓	✓	x	x
Analytics (Analytique)				

Tableau 4-5 : Autorisations prédéfinies (suite)

Autorisation	Administrateur	Développeur de méthode	Analyst	Examineur
New results (Nouveaux résultats)	✓	✓	✓	×
Create processing method (Créer une méthode de traitement)	✓	✓	✓	×
Modify processing method (Modifier le méthode de traitement)	✓	✓	×	×
Allow Export and Create Report of unlocked Results Table (Autoriser l'exportation et la création d'un rapport du tableau de résultats déverrouillé)	✓	×	×	×
Save results for Automation Batch (Sauvegarder les résultats pour le lot d'automatisation)	✓	✓	✓	×
Change default quantitation method integration algorithm (Modifier l'algorithme d'intégration de la méthode de quantification par défaut)	✓	✓	×	×
Change default quantitation method integration parameters (Modifier les paramètres d'intégration de la méthode de quantification par défaut)	✓	✓	×	×

Contrôle d'accès à Analyst

Tableau 4-5 : Autorisations prédéfinies (suite)

Autorisation	Administrateur	Développeur de méthode	Analyst	Examineur
Enable project modified peak warning (Activer l'avertissement de pic modifié du projet)	✓	×	×	×
Add samples (Ajouter des échantillons)	✓	✓	✓	×
Remove selected samples (Retirer les échantillons sélectionnés)	✓	✓	✓	×
Export, import, or remove external calibration (Exporter, importer ou supprimer un étalonnage externe)	✓	✓	✓	×
Modify sample name (Modifier le nom d'un échantillon)	✓	✓	✓	×
Modify sample type (Modifier le type d'échantillon)	✓	✓	✓	×
Modify sample ID (Modifier l'ID d'un échantillon)	✓	✓	✓	×
Modify actual concentration (Modifier la concentration réelle)	✓	✓	✓	×
Modify dilution factor (Modifier le facteur de dilution)	✓	✓	✓	×
Modify comment fields (Modifier les champs de commentaires)	✓	✓	✓	×
Enable manual integration (Activer l'intégration manuelle)	✓	✓	✓	×

Tableau 4-5 : Autorisations prédéfinies (suite)

Autorisation	Administrateur	Développeur de méthode	Analyst	Examineur
Set peak to not found (Définir le pic sur Introuvable)	✓	✓	✓	×
Include or exclude a peak from the results table (Inclure ou exclure un pic du tableau de résultats)	✓	✓	✓	×
Regression options (Options de régression)	✓	✓	✓	×
Modify results table integration parameters for a single chromatogram (Modifier les paramètres d'intégration des tableaux de résultats pour un chromatogramme unique)	✓	✓	✓	×
Modify quantitation method for the results table component (Modifier la méthode de quantification pour le composant du tableau de résultats)	✓	✓	✓	×
Create metric plot new settings (Créer de nouveaux paramètres de graphique métrique)	✓	✓	✓	✓
Add custom columns (Ajouter des colonnes personnalisées)	✓	✓	✓	×

Contrôle d'accès à Analyst

Tableau 4-5 : Autorisations prédéfinies (suite)

Autorisation	Administrateur	Développeur de méthode	Analyst	Examineur
Set peak review title format (Définir le format du titre de l'examen de pic)	✓	x	x	x
Remove custom column (Supprimer la colonne personnalisée)	✓	✓	x	x
Results table display settings (Paramètres d'affichage du tableau de résultats)	✓	✓	✓	✓
Lock results table (Verrouiller le tableau de résultats)	✓	✓	✓	✓
Unlock results table (Déverrouiller le tableau de résultats)	✓	x	x	x
Mark results file as reviewed and save (Marquer le fichier de résultats comme révisé et l'enregistrer)	✓	x	x	✓
Modify report template (Modifier le modèle de rapport)	✓	✓	x	x
Transfer results to LIMS (Transférer les résultats vers LIMS)	✓	✓	✓	x
Modify barcode column (Modifier la colonne de code-barres)	✓	✓	x	x
Change comparison sample assignment (Modifier l'affectation de l'échantillon de comparaison)	✓	✓	x	x

Tableau 4-5 : Autorisations prédéfinies (suite)


Autorisation	Administrateur	Développeur de méthode	Analyst	Examineur
Add the MSMS spectra to library (Ajouter les spectres MSMS à la bibliothèque)	✓	✓	×	×
Project default settings (Paramètres par défaut du projet)	✓	✓	×	×
Create report in all formats (Créer un rapport sous tous les formats)	✓	✓	✓	✓
Edit flagging criteria parameters (Modifier les paramètres des critères de marquage)	✓	✓	✓	×
Automatic outlier removal parameter change (Modifier les paramètres de suppression automatique des données aberrantes)	✓	✓	×	×
Enable automatic outlier removal (Activer la suppression automatique des données aberrantes)	✓	✓	✓	×
Update processing method via FF/LS (Mettre à jour la méthode de traitement via FF/LS)	✓	✓	×	×
Update results via FF/LS (Mettre à jour les résultats via FF/LS)	✓	✓	×	×

Tableau 4-5 : Autorisations prédéfinies (suite)

Autorisation	Administrateur	Développeur de méthode	Analyst	Examineur
Enable grouping by adducts functionality (Activer la fonction de regroupement par adduits)	✓	✓	×	×
Browse for files (Naviguer vers les fichiers)	✓	✓	✓	✓
Enable standard addition (Activer l'ajout standard)	✓	✓	✓	×
Set Manual Integration Percentage Rule (Définir la règle de pourcentage d'intégration manuelle)	✓	×	×	×

Gérer les utilisateurs

Ajouter un utilisateur ou un groupe

1. Ouvrez l'espace de travail Configuration.
2. Ouvrez la page User Management.
3. Ouvrez l'onglet Users.
4. Cliquez sur **Add User** ().
- La boîte de dialogue Select User or Group 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 Select User or Group et son utilisation, appuyez sur **F1**.

6. Pour que l'utilisateur soit actif, vérifiez que la case **Active user or group** soit bien cochée.
7. Dans la section **Roles**, sélectionnez un ou plusieurs rôles, puis cliquez sur **Save**.

Désactiver des utilisateurs ou des groupes

1. Ouvrez l'espace de travail Configuration.
2. Ouvrez la page User Management.

3. Ouvrez l'onglet Users.
4. Dans la liste **User name or group**, sélectionnez l'utilisateur ou le groupe à désactiver.
5. Décochez la case **Active user or group**.
Le logiciel demande votre confirmation.
6. Cliquez sur **Yes**.

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 de SCIEX OS.

1. Ouvrez l'espace de travail Configuration.
2. Ouvrez la page User Management.
3. Ouvrez l'onglet Users.
4. Dans la liste **User name or group**, sélectionnez l'utilisateur ou le groupe à supprimer.
5. Cliquez sur **Delete**.
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 User Management.
3. Ouvrez l'onglet Users.
4. Dans le champ **User name or group**, 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 **Save**.

Créer un rôle personnalisé

1. Ouvrez l'espace de travail Configuration.
2. Ouvrez la page User Management.
3. Ouvrez l'onglet Roles.
4. Cliquez sur **Add Role** ().
La boîte de dialogue Duplicate a User Role s'ouvre.

Contrôle d'accès à Analyst

5. Dans le champ **Existing user role**, 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 **Save All Roles**.
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 User Management.
3. Ouvrez l'onglet Roles.
4. Cliquez sur **Delete a Role**.
La boîte de dialogue Delete a User Role 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 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 User Management.
3. Cliquez sur **Advanced > Export User Management settings**.
La boîte de dialogue Export User Management Settings apparaît.
4. Cliquez sur **Browse**.
5. Naviguez jusqu'au dossier contenant les paramètres à sauvegarder, sélectionnez-le puis cliquez sur **Select Folder**.
6. Cliquez sur **Export**.

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 User Management.
3. Cliquez sur **Advanced > Import User Management settings**.
La boîte de dialogue Import User Management Settings apparaît.
4. Cliquez sur **Browse**.
5. Naviguez jusqu'au fichier contenant les paramètres à importer, sélectionnez-le puis cliquez sur **Open**.
Le logiciel vérifie la validité du fichier.
6. Cliquez sur **Import**.
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 réglages 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 User Management.
3. Cliquez sur **Advanced > Restore previous settings**.
La boîte de dialogue Restore User Management Settings apparaît.
4. Cliquez sur **Yes**.
5. Fermez puis ouvrez de nouveau SCIEX OS.

Configurer l'accès aux projets et aux fichiers de projets

Utilisez les fonctions de sécurité Windows pour contrôler l'accès au dossier SCIEX OS Data. Par défaut, les fichiers du 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, voir le tableau : [Tableau 4-6](#).

Tableau 4-6 : Dossiers du projet

Dossier	Table des matières
\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.
\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 les types de fichiers courants du logiciel SCIEX OS, voir le tableau : [Tableau 4-7](#).

Tableau 4-7 : Fichiers SCIEX OS

Extension	Type de fichier	Dossier
atds	<ul style="list-style-type: none">Données et archives du registre d'audit du poste de travailParamètres du registre d'audit du poste de travailDonnées du registre d'audit du projet et archivesParamètres du registre d'audit du projet	<ul style="list-style-type: none">Pour les projets : <code><project name>\Audit Data</code>Pour le poste de travail : <code>C:\ProgramData\SCIEX\Audit Data</code>

Tableau 4-7 : Fichiers SCIEX OS (suite)

Extension	Type de fichier	Dossier
atms	Cartes d'audit	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Optimization • Data
exml	Project default settings	Project Information
journal	Fichiers temporaires créés par SCIEX OS	Dossiers divers
lcm	Méthode LC	Acquisition Methods
msm	Méthode MS	Acquisition Methods
pdf	Données du document portable	—
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 Remarque : SCIEX OS ne peut ouvrir que les fichiers qsession créés avec SCIEX OS.	Quantitation Results
wiff	Fichier de données du spectromètre de masse compatible avec le logiciel SCIEX OS Remarque : SCIEX OS génère les fichiers wiff et wiff2.	Data

Tableau 4-7 : Fichiers SCIEX OS (suite)

Extension	Type de fichier	Dossier
wiff.scan	Fichier de données du spectromètre de masse	<ul style="list-style-type: none">• Optimization• Data
wiff2	Fichier de données du spectromètre de masse généré par SCIEX OS	<ul style="list-style-type: none">• Optimization• Data
xls ouxlsx	Feuille de calcul Excel	Batch
xps	Réétalonnage	Data\Cal

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 SCIEX OS ne peuvent pas être installés sur le même poste de travail.


Utilisateurs

Utilisez la page User Management pour ajouter des utilisateurs et groupes Windows à la base de données de gestion des utilisateurs pour SCIEX OS. L'administrateur peut également ajouter, modifier et supprimer des rôles d'utilisateurs 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 à SCIEX OS lorsque 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 Central Administration.
2. Ouvrez la page User Management.
3. Ouvrez l'onglet User Pool.
4. Cliquez sur **Add users to the User Pool** ().
- La boîte de dialogue Select Users or Groups s'ouvre.
5. Saisissez le nom d'un utilisateur ou d'un groupe, puis cliquez sur **OK**.

Central Administrator Console

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 Central Administration.
2. Ouvrez la page User Management.
3. Ouvrez l'onglet User Pool.
4. Dans le volet de droite, sélectionnez l'utilisateur ou le groupe à supprimer, puis cliquez sur **Delete**.
Le logiciel demande votre confirmation.
5. Cliquez sur **OK**.

Rôles utilisateur et autorisations

Cette section décrit la page User Roles and Permissions.

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 rôles déterminent les fonctions accessibles à l'utilisateur. Les rôles prédéfinis ne peuvent pas être supprimés et leurs autorisations ne peuvent pas être modifiées.

Tableau 5-1 : Rôles prédéfinis

Rôle	Tâches habituelles
Administrator (Administrateur)	<ul style="list-style-type: none">• Gère le système.• Configure la sécurité.
Method Developer (Développeur de méthode)	<ul style="list-style-type: none">• Crée des méthodes.• Exécute des lots.• Analyse les données à utiliser par l'utilisateur final.
Analyst (Analyst)	<ul style="list-style-type: none">• Exécute des lots.• Analyse les données à utiliser par l'utilisateur final.
Reviewer (Réviseur)	<ul style="list-style-type: none">• Examine les données.• Examine les registres d'audit.• Examine les résultats de quantification.

Tableau 5-2 : Autorisations prédéfinies

Autorisation	Administra- teur	Développeur de méthode	Analyst	Examineur
Batch (Lot)				

Tableau 5-2 : Autorisations prédéfinies (suite)

Autorisation	Administrateur	Développeur de méthode	Analyst	Examineur
Submit unlocked methods (Soumettre les méthodes déverrouillées)	✓	✓	✓	×
Open (Ouvrir)	✓	✓	✓	✓
Save as (Enregistrer sous)	✓	✓	✓	×
Submit (Envoyer)	✓	✓	✓	×
Save (Enregistrer)	✓	✓	✓	×
Save ion reference table (Enregistrer le tableau de référence d'ions)	✓	✓	✓	×
Add data sub-folders (Ajouter des sous-dossiers de données)	✓	✓	✓	×
Configure Decision Rules (Configurer les règles de décision)	✓	✓	✓	×
Configuration (Configuration)				
General tab (Onglet General)	✓	✓	×	×
General: change regional setting (Général : modifier le paramètre régional)	✓	✓	×	×
General: full screen mode (Général : mode plein écran)	✓	✓	×	×
LIMS communication tab (Onglet Communication LIMS)	✓	✓	×	×
General: Stop Windows services (Général : arrêter les services Windows)	✓	×	×	×

Tableau 5-2 : Autorisations prédéfinies (suite)

Autorisation	Administrateur	Développeur de méthode	Analyst	Examineur
Audit maps tab (Onglet Cartes d'audit)	✓	×	×	×
Queue tab (Onglet File d'attente)	✓	✓	✓	✓
Queue: instrument idle time (File d'attente : période d'inactivité de l'instrument)	✓	✓	×	×
Queue: max number of acquired samples (File d'attente : nombre max. d'échantillons acquis)	✓	✓	×	×
Queue: other queue settings (File d'attente : autres paramètres de file d'attente)	✓	✓	×	×
Projects tab (Onglet Projets)	✓	✓	✓	✓
Projects: create project (Projets : créer projet)	✓	✓	✓	×
Projects: apply an audit map template to an existing project (Projets : appliquer un modèle de carte d'audit à un projet existant)	✓	×	×	×
Projects: create root directory (Projets : créer un répertoire racine)	✓	×	×	×
Projects: set current root directory (Projets : définir le répertoire racine actuel)	✓	×	×	×

Tableau 5-2 : Autorisations prédéfinies (suite)

Autorisation	Administra- teur	Développeur de méthode	Analyst	Examineur
Projects: specify network credentials (Projets : spécifier les identifiants du réseau)	✓	×	×	×
Projects: Enable checksum writing for wiff1 data creation (Projets : activer l'écriture de somme de contrôle pour la création de données wiff1)	✓	×	×	×
Projects: clear root directory (Projets : effacer un répertoire racine)	✓	×	×	×
Devices tab (Onglet Appareils)	✓	✓	✓	×
User management tab (Onglet Gestion des utilisateurs)	✓	×	×	×
Force user logoff (Forcer la déconnexion des utilisateurs)	✓	×	×	×
Event Log (Registre des événements)				
Access event log workspace (Accéder à l'espace de travail du registre des événements)	✓	✓	✓	✓
Archive log (Registre d'archive)	✓	✓	✓	✓
Audit Trail (Registre d'audit)				
Access audit trail workspace (Accéder à l'espace de travail du registre d'audit)	✓	✓	✓	✓

Tableau 5-2 : Autorisations prédéfinies (suite)

Autorisation	Administrateur	Développeur de méthode	Analyst	Examineur
View active audit map (Afficher la carte d'audit active)	✓	✓	✓	✓
Print/Export audit trail (Imprimer/Exporter le registre d'audit)	✓	✓	✓	✓
Data Acquisition Panel (Volet Data Acquisition)				
Start (Démarrer)	✓	✓	✓	×
Stop (Arrêter)	✓	✓	✓	×
Save (Enregistrer)	✓	✓	✓	×
MS & LC Method (Méthodes MS et LC)				
Access method workspace (Accéder à l'espace de travail de méthode)	✓	✓	✓	✓
New (Nouveau)	✓	✓	×	×
Open (Ouvrir)	✓	✓	✓	✓
Save (Enregistrer)	✓	✓	×	×
Save as (Enregistrer sous)	✓	✓	×	×
Lock/Unlock method (Verrouiller/Déverrouiller la méthode)	✓	✓	×	×
Queue (File d'attente)				
Manage (Gestion)	✓	✓	✓	×
Start/Stop (Démarrer/Arrêter)	✓	✓	✓	×
Print (Imprimer)	✓	✓	✓	✓
Library (Bibliothèque)				
Access library workspace (Accéder à l'espace de travail Bibliothèque)	✓	✓	✓	✓

Tableau 5-2 : Autorisations prédéfinies (suite)

Autorisation	Administra- teur	Développeur de méthode	Analyst	Examineur
CAC settings (Client CAC)				
Enable Central Administration (Activer Central Administration)	✓	×	×	×
MS Tune (Réglage MS)				
Access MS Tune workspace (Accéder à l'espace de travail Réglage MS)	✓	✓	✓	×
Advanced MS Tuning (Réglage MS avancé)	✓	✓	×	×
Advanced troubleshooting (Dépannage avancé)	✓	✓	×	×
Quick status check (Contrôle d'état rapide)	✓	✓	✓	×
Restore instrument data (Restaurer les données de l'instrument)	✓	✓	×	×
Analytics (Analytique)				
New results (Nouveaux résultats)	✓	✓	✓	×
Create processing method (Créer une méthode de traitement)	✓	✓	✓	×
Modify processing method (Modifier le méthode de traitement)	✓	✓	×	×
Allow Export and Create Report of unlocked Results Table (Autoriser l'exportation et la création d'un rapport du tableau de résultats déverrouillé)	✓	×	×	×

Tableau 5-2 : Autorisations prédéfinies (suite)

Autorisation	Administra- teur	Développeur de méthode	Analyst	Examineur
Save results for Automation Batch (Sauvegarder les résultats pour le lot d'automatisation)	✓	✓	✓	×
Change default quantitation method integration algorithm (Modifier l'algorithme d'intégration de la méthode de quantification par défaut)	✓	✓	×	×
Change default quantitation method integration parameters (Modifier les paramètres d'intégration de la méthode de quantification par défaut)	✓	✓	×	×
Enable project modified peak warning (Activer l'avertissement de pic modifié du projet)	✓	×	×	×
Add samples (Ajouter des échantillons)	✓	✓	✓	×
Remove selected samples (Retirer les échantillons sélectionnés)	✓	✓	✓	×
Export, import, or remove external calibration (Exporter, importer ou supprimer un étalonnage externe)	✓	✓	✓	×
Modify sample name (Modifier le nom d'un échantillon)	✓	✓	✓	×

Tableau 5-2 : Autorisations prédéfinies (suite)

Autorisation	Administrateur	Développeur de méthode	Analyst	Examineur
Modify sample type (Modifier le type d'échantillon)	✓	✓	✓	×
Modify sample ID (Modifier l'ID d'un échantillon)	✓	✓	✓	×
Modify actual concentration (Modifier la concentration réelle)	✓	✓	✓	×
Modify dilution factor (Modifier le facteur de dilution)	✓	✓	✓	×
Modify comment fields (Modifier les champs de commentaires)	✓	✓	✓	×
Enable manual integration (Activer l'intégration manuelle)	✓	✓	✓	×
Set peak to not found (Définir le pic sur Introuvable)	✓	✓	✓	×
Include or exclude a peak from the results table (Inclure ou exclure un pic du tableau de résultats)	✓	✓	✓	×
Regression options (Options de régression)	✓	✓	✓	×

Tableau 5-2 : Autorisations prédéfinies (suite)

Autorisation	Administra- teur	Développeur de méthode	Analyst	Examineur
Modify results table integration parameters for a single chromatogram (Modifier les paramètres d'intégration des tableaux de résultats pour un chromatogramme unique)	✓	✓	✓	×
Modify quantitation method for the results table component (Modifier la méthode de quantification pour le composant du tableau de résultats)	✓	✓	✓	×
Create metric plot new settings (Créer de nouveaux paramètres de graphique métrique)	✓	✓	✓	✓
Add custom columns (Ajouter des colonnes personnalisées)	✓	✓	✓	×
Set peak review title format (Définir le format du titre de l'examen de pic)	✓	×	×	×
Remove custom column (Supprimer la colonne personnalisée)	✓	✓	×	×
Results table display settings (Paramètres d'affichage du tableau de résultats)	✓	✓	✓	✓
Lock results table (Verrouiller le tableau de résultats)	✓	✓	✓	✓

Tableau 5-2 : Autorisations prédéfinies (suite)

Autorisation	Administrateur	Développeur de méthode	Analyst	Examineur
Unlock results table (Déverrouiller le tableau de résultats)	✓	×	×	×
Mark results file as reviewed and save (Marquer le fichier de résultats comme révisé et l'enregistrer)	✓	×	×	✓
Modify report template (Modifier le modèle de rapport)	✓	✓	×	×
Transfer results to LIMS (Transférer les résultats vers LIMS)	✓	✓	✓	×
Modify barcode column (Modifier la colonne de code-barres)	✓	✓	×	×
Change comparison sample assignment (Modifier l'affectation de l'échantillon de comparaison)	✓	✓	×	×
Add the MSMS spectra to library (Ajouter les spectres MSMS à la bibliothèque)	✓	✓	×	×
Project default settings (Paramètres par défaut du projet)	✓	✓	×	×
Create report in all formats (Créer un rapport sous tous les formats)	✓	✓	✓	✓
Edit flagging criteria parameters (Modifier les paramètres des critères de marquage)	✓	✓	✓	×

Tableau 5-2 : Autorisations prédéfinies (suite)


Autorisation	Administrateur	Développeur de méthode	Analyst	Examineur
Automatic outlier removal parameter change (Modifier les paramètres de suppression automatique des données aberrantes)	✓	✓	×	×
Enable automatic outlier removal (Activer la suppression automatique des données aberrantes)	✓	✓	✓	×
Update processing method via FF/LS (Mettre à jour la méthode de traitement via FF/LS)	✓	✓	×	×
Update results via FF/LS (Mettre à jour les résultats via FF/LS)	✓	✓	×	×
Enable grouping by adducts functionality (Activer la fonction de regroupement par adduits)	✓	✓	×	×
Browse for files (Naviguer vers les fichiers)	✓	✓	✓	✓
Enable standard addition (Activer l'ajout standard)	✓	✓	✓	×
Set Manual Integration Percentage Rule (Définir la règle de pourcentage d'intégration manuelle)	✓	×	×	×
Explorer (Explorer)				

Tableau 5-2 : Autorisations prédéfinies (suite)

Autorisation	Administrateur	Développeur de méthode	Analyst	Examineur
Access explorer workspace (Accéder à l'espace de travail Explorer)	✓	✓	✓	✓
Export (Exporter)	✓	✓	✓	×
Print (Imprimer)	✓	✓	✓	×
Options (Options)	✓	✓	✓	×
Recalibrate (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.

- Ouvrez l'espace de travail Central Administration.
- Ouvrez la page User Management.
- Ouvrez l'onglet User Roles and Permissions.
- Cliquez sur **Add Role** ().
La boîte de dialogue Duplicate a User Role s'ouvre.
- Dans le champ **Existing user role**, sélectionnez le rôle à utiliser comme modèle pour le nouveau rôle.
- Entrez un nom et une description pour le rôle, puis cliquez sur **OK**.
Le nouveau rôle est affiché dans la fenêtre User Roles and Permission Categories.
- Sélectionnez les privilèges d'accès pour le rôle en cochant les cases appropriées.
- Cliquez sur **Save All Roles**.

Supprimer un rôle personnalisé

- Ouvrez l'espace de travail Central Administration.
- Ouvrez la page User Management.
- Ouvrez l'onglet User Roles and Permissions.
- Cliquez sur **Delete a Role**.
La boîte de dialogue Delete a User Role s'ouvre.
- Sélectionnez le rôle à supprimer, puis cliquez sur **OK**.

Groupes de travail

Utilisez la page Workgroup Management 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 un 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 précis, gérez la sécurité de ce poste en local avec SCIEX OS.

Créer un groupe de travail

1. Ouvrez l'espace de travail Central Administration.
2. Ouvrez la page Workgroup Management.
3. Cliquez sur **Add Workgroup** ().
La boîte de dialogue Add a Workgroup apparaît.
4. Saisissez un nom dans le champ **Workgroup Name**.
5. Saisissez une description dans le champ **Description**, puis cliquez sur **Add**.
Le groupe de travail est créé et ajouté au volet Manage Workgroups and Assignments. 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 Central Administration.
2. Ouvrez la page Workgroup Management.
3. Développez la liste **Workgroups** et repérez le groupe de travail à supprimer. Cliquez sur **Delete**.
La boîte de dialogue Delete Workgroup apparaît.
4. Cliquez sur **Yes**.

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 Central Administration.
2. Ouvrez la page Workgroup Management.
3. Dans le volet Manage Workgroups and Assignments, développez le groupe de travail à modifier puis développez la liste **Users**.
4. Sélectionnez un utilisateur ou un groupe et cliquez sur **Add** ().

Conseil ! Ajoutez ou sélectionnez des utilisateurs multiples en appuyant sur **Shift** 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 **Save**.

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 Central Administration.
2. Ouvrez la page Workgroup Management.
3. Dans le volet Manage Workgroups and Assignments, développez le groupe de travail à modifier puis développez la liste **Users**.

Central Administrator Console

4. Dans la section Current Workgroup Membership, affectez ou retirez des rôles dans la colonne **Assign Roles**.
5. Cliquez sur **Save**.

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 Central Administration.
2. Ouvrez la page Workgroup Management.
3. Dans le volet Manage Workgroups and Assignments, développez le groupe de travail à modifier puis développez la liste **Workstations**.
4. Sélectionnez un poste de travail et cliquez sur **Add** ().
Le poste de travail est ajouté au groupe de travail actuel.
5. Cliquez sur **Save**.

Attribuer des paramètres de sécurité de groupe de travail

Procédures préalables
<ul style="list-style-type: none">• 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 Security Mode](#).

1. Ouvrez l'espace de travail Central Administration.
2. Ouvrez la page Workgroup Management.
3. Dans le volet Manage Workgroups and Assignments, développez le groupe de travail à modifier puis développez la liste **Workstations**.
4. (Facultatif) Pour définir le groupe de travail actuel comme groupe de travail par défaut pour ce poste de travail, cochez la case **Set Default** dans la section Current Workgroup Membership.
5. Dans la section Assign Security Settings, sélectionnez le **Security mode** pour le groupe de travail puis saisissez les durées **Screen lock** et **Auto logoff** appropriées.
6. Cliquez sur **Save**.

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 Central Administration.
2. Ouvrez la page Workgroup Management.
3. Dans le volet Manage Workgroups and Assignments, développez le groupe de travail à modifier puis développez la liste **Projects**.
4. Cochez la case **Use central settings for projects**.
La section de sélection des projets est affichée.
5. Sélectionnez un **Project root directory** 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 **Add** () pour ajouter les projets au groupe de travail.
La racine du projet est ajoutée au tableau Current Workgroup Membership. Développez la racine du projet pour afficher les projets actuels dans le groupe de travail.
7. Cliquez sur **Save**.

Gérer des projets

Utilisez la page Project Management 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 Project Root Pool 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 Project Root Pool est synchronisé avec le contenu des racines du 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 Central Administration.
2. Ouvrez la page Project Management.
3. Cliquez sur **Add new or existing project root to project pool** ().
La boîte de dialogue Add Root Directory apparaît.
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 **Browse**, 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 : Pour les installations SCIEX OS 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 Central Administration.
2. Ouvrez la page Project Management.
3. Repérez le répertoire racine de projet à supprimer et cliquez sur **Delete Project Root** dans la section Actions.
Le logiciel demande votre confirmation.
4. Cliquez sur **OK**.

Ajouter un projet

Procédures préalables
<ul style="list-style-type: none">• 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 Central Administration.
2. Ouvrez la page Project Management.
3. Cliquez sur **Add project** dans la section Actions du dossier racine. La boîte de dialogue New Project apparaît.
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 Central Administration.
2. Ouvrez la page Project Management.
3. Cliquez sur **Add data sub-folders** dans la section Actions du dossier racine. La boîte de dialogue Add Data Sub-Folders apparaît.
4. Sélectionnez un projet auquel appartiendra le sous-dossier.
5. Cliquez sur **Add a new data sub-folder** ().
La boîte de dialogue Data Sub-Folder Name s'ouvre.
6. Saisissez le nom du sous-dossier.
7. Cliquez sur **Save**.

Conseil ! Les sous-dossiers peuvent être imbriqués dans d'autres sous-dossiers. Pour créer un sous-dossier imbriqué, sélectionnez un sous-dossier existant dans la section

Project Data Sub-Folders puis cliquez sur **Add a new data sub-folder** ().


8. Fermez la boîte de dialogue Add Data Sub-Folders.

Postes de travail

Utilisez la page Workstation Management pour gérer tous les postes de travail connectés au serveur CAC. Des paramètres personnalisés sont automatiquement appliqués aux postes de travail sous le contrôle du logiciel CAC.

Ajouter un poste de travail

Sur la page Workstation Management, les administrateurs peuvent ajouter ou retirer des postes de travail du contrôle du logiciel Central Administrator Console (CAC).

1. Ouvrez l'espace de travail Central Administration.
2. Ouvrez la page Workstation Management.
3. Cliquez sur **Add Workstation to the Workstations Pool** ().
La boîte de dialogue Select Computers s'ouvre.
4. Saisissez les noms des postes de travail à ajouter et cliquez sur **OK**.

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 du groupe de postes de travail. La suppression d'un poste de travail le retire de tous les groupes de travail auxquels il était attribué. Aucune donnée n'est perdue sur le poste de travail lors de sa suppression.

1. Ouvrez l'espace de travail Central Administration.
2. Ouvrez la page Workstation Management.
3. Cliquez sur **Workstation Management**.
4. Dans le volet Workstation Pool, repérez le poste de travail à supprimer, puis cliquez sur **Delete**.
La boîte de dialogue Delete Workstation apparaît.
5. Cliquez sur **OK**.

Rapports et fonctions de sécurité

Générer des rapports de données de groupe de travail

Les utilisateurs peuvent générer des rapports de données avec des détails tels que les utilisateurs, rôles, postes de travail, projets et groupes de travail configurés.

1. Ouvrez l'espace de travail Central Administration.
2. Cliquez sur **Print**.
La boîte de dialogue Print s'ouvre.
3. Définissez les options d'impression et cliquez sur **Print**.

4. (Imprimer sur PDF uniquement) Naviguez jusqu'à l'emplacement d'enregistrement du rapport et cliquez sur **Save**.

Exporter les paramètres du logiciel de CAC

L'utilisateur peut exporter les paramètres de sécurité applicables à un autre serveur Central Administrator Console (CAC). Les paramètres sont exportés sous la forme d'un fichier ecac.

1. Ouvrez l'espace de travail Central Administration.
2. Cliquez sur **Advanced > Export CAC settings**.
La boîte de dialogue Export CAC Settings apparaît.
3. Cliquez sur **Browse**.
4. Naviguez jusqu'au dossier contenant les paramètres à sauvegarder, sélectionnez-le puis cliquez sur **Select Folder**.
5. Cliquez sur **Export**.
Un message de confirmation apparaît, avec le nom du fichier contenant les paramètres exportés.
6. Cliquez sur **OK**.

Importer les paramètres du logiciel de CAC

Procédures préalables
<ul style="list-style-type: none">• Exporter les paramètres du logiciel de CAC

L'utilisateur ne peut pas importer les paramètres de sécurité de SCIEX OS ou d'autres serveurs Central Administrator Console (CAC). Les paramètres sont importés depuis un fichier ecac.

1. Ouvrez l'espace de travail Central Administration.
2. Cliquez sur **Advanced > Import CAC settings**.
La boîte de dialogue Import CAC Settings apparaît.
3. Cliquez sur **Browse**.
4. Naviguez jusqu'au fichier contenant les paramètres à importer, sélectionnez-le puis cliquez sur **Open**.
Le logiciel vérifie la validité du fichier.
5. Cliquez sur **Import**.
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**.

Restaurer les paramètres logiciels CAC

L'utilisateur peut automatiquement importer les derniers paramètres ecac exportés.

1. Ouvrez l'espace de travail Central Administration.
2. Cliquez sur **Advanced > Restore CAC settings**.
La boîte de dialogue Export CAC Settings apparaît.

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

3. Cliquez sur **Yes**.

Cette section décrit le fonctionnement de l'acquisition réseau dans SCIEX OS et les avantages et limites des projets sur le 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. Toutefois, sans accès en suppression à ce dossier, SCIEX OS ne peut pas fonctionner de manière optimale. 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.
- Être dans la base de données de gestion des utilisateurs SCIEX OS.

Le compte SNA est spécifié sur la page Project 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, SCIEX OS utilise les identifiants de l'utilisateur actuellement 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 commence par écrire chaque échantillon dans un dossier sur le disque 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 devient 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 périodes prolongées de perte 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 SCIEX OS stocke les données. Pour être certain que les informations relatives au projet sont stockées en toute sécurité, créez le répertoire racine à l'aide de SCIEX OS. Ne créez pas de projets dans File Explorer.

Éventuellement, lorsque vous créez des répertoires racines sur une ressource réseau, définissez les identifiants **Credentials for Secure Network Account**. Il s'agit du compte réseau sécurisé défini sur la ressource en réseau. Consulter 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 **Projects**.
3. Dans la section **Advanced**, cliquez sur **Credentials for Secure Network Account**.
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**.

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

Les événements audités sont stockés dans des registres d'audit. Deux types de registres d'audit sont disponibles : poste de travail et projet.

Les registres d'audit de poste de travail sont des fichiers qui conservent les événements audités pour l'ordinateur sur lequel SCIEX OS ou le logiciel Central Administrator Console (CAC) est exécuté. Pour obtenir une liste complète des événements audités, consultez la section [Registre d'audit du poste de travail](#).

Un registre d'audit de projet est le fichier qui conserve les événements audités pour le projet. Pour obtenir une liste complète des événements audités, consultez la section [Registre d'audit du projet](#). Dans SCIEX OS et dans le logiciel CAC, l'espace de travail Audit Trail présente les registres d'audit pour les projets dans le répertoire racine actuel. Les événements du registre d'audit de traitement sont contenus dans la carte du registre d'audit du projet. Ils sont stockés avec le tableau de résultats.

Les registres d'audit, associés à des fichiers tels que des fichiers wiff2 et des tableaux de résultats, constituent 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)	<ul style="list-style-type: none">• Modifications apportées :• Attribution de la carte d'audit active• Réglage de l'instrument• Files d'attente d'échantillons• Sécurité• Ajustement• Appareils	<ul style="list-style-type: none">• Dossier C:\ProgramData\SCIEX\ Audit Data	<ul style="list-style-type: none">• Pas de carte d'audit

Tableau 7-1 : Registres d'audit (suite)

Registre d'audit	Exemples d'événements enregistrés	Cartes d'audit disponibles enregistrées dans	Cartes d'audit par défaut
Poste de travail (CAC)	<ul style="list-style-type: none"> • Modifications apportées : <ul style="list-style-type: none"> • Carte d'audit • Serveur CAC • Sécurité • Registre d'utilisateurs 	<ul style="list-style-type: none"> • Dossier C:\ProgramData\SCIEX\Audit Data 	<ul style="list-style-type: none"> • Carte d'audit silencieuse
Projet (un par projet)	<ul style="list-style-type: none"> • Modifications apportées : <ul style="list-style-type: none"> • Attribution de la carte d'audit active (SCIEX OS) • Projet • Data • Impression 	<ul style="list-style-type: none"> • Dossier <project>\Audit Data 	<ul style="list-style-type: none"> • Spécifié sur la page Audit Maps de l'espace de travail Configuration

Quand le registre d'audit du poste de travail ou d'un projet contient 20 000 enregistrements d'audit, SCIEX OS et le logiciel CAC archivent automatiquement les enregistrements et démarre 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. Deux types de cartes d'audit sont disponibles : poste de travail 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 pour un projet peut être éditée dans SCIEX OS ou dans le logiciel Central Administrator Console (CAC).

Audit

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

Quand le logiciel SCIEX OS est installé, la carte d'audit par défaut pour 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. Voir 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 adaptées aux procédures de fonctionnement standard. Plusieurs modèles de carte d'audit sont disponibles par défaut lors de l'installation du logiciel, mais il peut s'avérer nécessaire de créer une carte personnalisée. Assurez-vous de disposer d'une carte d'audit adaptée au registre d'audit du poste de travail et d'une carte d'audit adaptée à chaque projet.

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

Tâche	Consulter
Créer une carte d'audit pour le registre d'audit du poste de travail.	<ul style="list-style-type: none">• Créer une carte d'audit de poste de travail.• Modifier une carte d'audit de poste de travail.
Appliquer la carte d'audit au registre d'audit du poste de travail.	<ul style="list-style-type: none">• Modifier la carte d'audit active d'un poste de travail.
Créer une carte d'audit active par défaut pour de nouveaux projets.	<ul style="list-style-type: none">• Créer une carte d'audit de projet.
Configurer la carte d'audit à utiliser pour chaque projet existant.	<ul style="list-style-type: none">• Créer une carte d'audit de projet.• Modifier une carte d'audit de projet.
Appliquer une carte d'audit à chaque projet existant.	<ul style="list-style-type: none">• 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.

Tableau 7-3 : Cartes d'audit installées (suite)

Carte d'audit	Description
Carte d'audit complète	Tous les événements sont audités. Des signatures électroniques et des motifs sont nécessaires pour l'ensemble des événements.
Pas de carte d'audit	Aucun événement n'est audité. Remarque : L'événement Change Active Audit Map Assignment est toujours enregistré, même si le modèle Pas de carte d'audit est utilisé.
Carte d'audit silencieuse	Tous les événements sont audités. Aucune signature électronique et aucun motif ne sont nécessaires pour les événements.

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

Pour obtenir des informations sur le processus d'audit, consultez le tableau : [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 une liste des événements du projet pouvant être audités, se reporter à la section : [Registre d'audit du projet](#).

Créer une carte d'audit de projet

1. Ouvrez l'espace de travail Configuration.
2. Cliquez sur **Audit Maps**.
3. Ouvrez l'onglet Projects Templates.
4. Dans le champ **Edit map template**, sélectionnez un modèle à utiliser comme base de la nouvelle carte.
5. Cliquez sur **Add Template** ().
La boîte de dialogue Add a Project Audit Map Template s'ouvre.

Audit

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 **Audited** pour l'événement.
 - b. (Facultatif) Si une raison est requise, sélectionnez **Reason Required**.
 - c. (Facultatif) Si une signature électronique est requise, sélectionnez **E-Sig Required**.
 - d. (Facultatif) Si des raisons prédéfinies sont requises, sélectionnez **Use Predefined Reason Only** et définissez les raisons.
8. Vérifiez que la case **Audited** ne soit cochée pour aucun des événements qui ne sera pas audité.
9. Cliquez sur **Save Template**.
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 **Yes**, sélectionnez les projets qui utiliseront cette nouvelle carte, puis cliquez sur **Apply**.
 - Si vous ne souhaitez pas appliquer la nouvelle carte à des projets existants, cliquez sur **No**.
11. (Facultatif) Pour utiliser cette carte d'audit comme carte d'audit par défaut pour tous les nouveaux projets, cliquez sur **Use as Default for New Projects**.

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 **Audit Maps**.
3. Ouvrez l'onglet Projects Templates.
4. Dans le champ **Edit map template**, sélectionnez la carte à modifier.
5. Sélectionnez et configurez les événements à enregistrer en respectant la procédure suivante :
 - a. Cochez la case **Audited** pour l'événement.
 - b. (Facultatif) Si une raison est requise, sélectionnez **Reason Required**.
 - c. (Facultatif) Si une signature électronique est requise, sélectionnez **E-Sig Required**.
 - d. (Facultatif) Si des raisons prédéfinies sont requises, sélectionnez **Use Predefined Reason Only** et définissez les raisons.
6. Vérifiez que la case **Audited** ne soit cochée pour aucun des événements qui ne sera pas audité.
7. Cliquez sur **Save Template**.
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 **Yes**, sélectionnez les projets qui utiliseront cette nouvelle carte, puis cliquez sur **Apply**.
 - Si vous ne souhaitez pas appliquer la nouvelle carte à des projets existants, cliquez sur **No**.

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 **Audit Maps**.
3. Ouvrez l'onglet Projects Templates.
4. Dans le champ **Edit map template**, sélectionnez la carte d'audit à attribuer au projet.
5. Cliquez sur **Apply to Existing Projects**.
La boîte de dialogue Apply Project Audit Map Template apparaît.
6. Cochez les cases correspondant aux projets auxquels appliquer cette carte d'audit.
7. Cliquez sur **Apply**.

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 **Audit Maps**.
3. Ouvrez l'onglet Projects Templates.
4. Dans le champ **Edit map template**, sélectionnez la carte à supprimer.
5. Cliquez sur **Delete Template**.
Le système demande votre confirmation.
6. Cliquez sur **Yes**.


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 une liste des événements du poste de travail pouvant être audités, se reporter à 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 **Audit Maps**.

Audit

3. Ouvrez l'onglet Workstation Templates.
4. Dans le champ **Edit map template**, sélectionnez un modèle à utiliser comme base de la nouvelle carte.
5. Cliquez sur **Add Template** ().
La boîte de dialogue Add a Workstation Audit Map Template 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 **Audited** pour l'événement.
 - b. (Facultatif) Si une raison est requise, sélectionnez **Reason Required**.
 - c. (Facultatif) Si une signature électronique est requise, sélectionnez **E-Sig Required**.
 - d. (Facultatif) Si des raisons prédéfinies sont requises, sélectionnez **Use Predefined Reason Only** et définissez les raisons.
8. Vérifiez que la case **Audited** ne soit cochée pour aucun des événements qui ne sera pas audité.
9. Cliquez sur **Save Template**.
10. (Facultatif) Pour utiliser cette carte d'audit comme carte d'audit active du poste de travail, cliquez sur **Apply to the Workstation**.

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 **Audit Maps**.
3. Ouvrez l'onglet Workstation Templates.
4. Dans le champ **Edit map template**, sélectionnez la carte à modifier.
5. Sélectionnez et configurez les événements à enregistrer en respectant la procédure suivante :
 - a. Cochez la case **Audited** pour l'événement.
 - b. (Facultatif) Si une raison est requise, sélectionnez **Reason Required**.
 - c. (Facultatif) Si une signature électronique est requise, sélectionnez **E-Sig Required**.
 - d. (Facultatif) Si des raisons prédéfinies sont requises, sélectionnez **Use Predefined Reason Only** et définissez les raisons.
6. Vérifiez que la case **Audited** ne soit cochée pour aucun des événements qui ne sera pas audité.
7. Cliquez sur **Save Template**.

-
8. (Facultatif) Pour utiliser cette carte d'audit comme carte active du poste de travail, cliquez sur **Apply to the Workstation**.

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 **Audit Maps**.
3. Ouvrez l'onglet Workstation Templates.
4. Dans le champ **Edit map template**, sélectionnez la carte à appliquer au poste de travail.
5. Cliquez sur **Apply to the Workstation**.

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 **Audit Maps**.
3. Ouvrez l'onglet Workstation Templates.
4. Dans le champ **Edit map template**, sélectionnez la carte à supprimer.
5. Cliquez sur **Delete Template**.
Le système demande votre confirmation.
6. Cliquez sur **Yes**.

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 un registre d'audit

1. Ouvrez l'espace de travail Audit Trail.
2. Sélectionnez le registre d'audit à afficher.
 - Pour afficher le registre d'audit du poste de travail, cliquez sur **Workstation**.
 - Pour afficher un registre d'audit de projet, sélectionnez le projet.
3. Pour afficher les détails d'un enregistrement d'audit, sélectionnez l'enregistrement.

Rechercher ou filtrer des enregistrements d'audit

1. Ouvrez l'espace de travail Audit Trail.
2. Sélectionnez le registre d'audit à rechercher.
3. Pour rechercher un registre d'audit spécifique, entrez du texte dans le champ **Find in 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 Filter Audit Trail apparaît.
 - b. Tapez les critères de filtre.
 - c. Cliquez sur **OK**.

Afficher un registre d'audit archivé

Une fois qu'un registre d'audit contient 20 000 enregistrements d'audit, SCIEX OS archive automatiquement les enregistrements et démarre un nouveau registre d'audit. Le nom des fichiers du registre d'audit archivé comporte 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-<nom du poste de travail>-<AAAA><MMJJHHMMSS>.atds

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

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

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

Imprimer un registre d'audit

1. Ouvrez l'espace de travail Audit Trail.
2. Sélectionnez le registre d'audit à imprimer.
3. Cliquez sur **Print**.
La boîte de dialogue Print apparaît.
4. Sélectionnez l'imprimante et cliquez sur **OK**.

Exporter les enregistrements du registre d'audit

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

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

Enregistrements dans le registre d'audit

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 7-4 : Champs des enregistrements d'événements

Champ	Description
Timestamp	Date et heure de l'enregistrement.
Event Name	Module qui a généré l'événement.
Description	Description de l'événement.
Reason	Raison de la modification telle que spécifiée par l'utilisateur, le cas échéant.
E-signature	Si une signature électronique a été fournie.
Full User Name	Nom de l'utilisateur.
Utilisateur	Nom principal de l'utilisateur (UPN).
Category	Type d'événement.

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](#).

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.

Audit

Les archives du registre d'audit du poste de travail sont stockées dans le dossier C:\ProgramData\SCIEX\Audit Data. Les noms de fichiers sont au format WorkstationAuditTrailData-<workstation name>-<YYYY><MMDDHHMMSS>.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, 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 Queue.
2. Arrêtez la file d'attente.
3. Annulez tous les échantillons restants dans le lot qui contient les échantillons à supprimer.
4. Fermez 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`.

Accéder aux données pendant des interruptions du réseau

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. Démarrez SCIEX OS.
Dans un délai de 15 minutes, 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.

Événements d'audit

B

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 pour les nouveaux projets créés dans le logiciel Central Administrator Console (CAC) est la **Silent Audit Map**.

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

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

SCIEX OS ou CAC	Logiciel Analyst
Espace de travail Analytics	
Actual Concentration changed	Événements de quantification : 'Concentration' a été modifié
Auto-Processing File saved	—
Barcode ID changed	—
Comparison sample changed in non-targeted workflow	—
Custom columns modified	Événements de quantification : 'Titre personnalisé' a été modifié
Data exploration opened	Événements du projet : le fichier de données a été ouvert
Data exported	—
Data transferred to LIMS	—
Dilution Factor changed	Événements de quantification : 'Facteur de dilution' a été modifié
External calibration changed	—
External calibration exported	—

Événements d'audit

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

SCIEX OS ou CAC	Logiciel Analyst
File saved	Événements du projet : le tableau de résultats de la quantification a été créé, le tableau de résultats de la quantification a été modifié, Événements du projet : le tableau de résultats a été sauvegardé
Formula column changed	Événements de quantification : Le nom de la formule a été modifié, Le nom de la formule a été ajouté, La chaîne de la formule a été modifiée, La colonne de la formule a été supprimée
Integration cleared	—
Integration parameters changed	Événements de quantification : le pic de quantification a été intégré
Library search result changed	—
Manual Integration	Événements de quantification : le pic de quantification a été intégré
Manual Integration reverted	Événements de quantification : Le pic de quantification est revenu à son état d'origine
MS/MS selection changed	—
Processing method changed and applied	Événements de quantification : la méthode de quantification a été modifiée
Report created	Événements du projet : impression d'un document sur l'imprimante, impression du document terminée sur l'imprimante
Results Table approved	Événements de quantification : l'examineur d'AQ a accédé à un tableau de résultats
Results Table created	Événements de quantification : un tableau de résultats a été créé
Results Table locked	—
Results Table unlocked	—
Sample ID changed	Événements de quantification : 'ID de l'échantillon' a été modifié
Sample Name changed	Événements de quantification : 'Nom de l'échantillon' a été modifié

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

SCIEX OS ou CAC	Logiciel Analyst
Samples added or removed	Événements de quantification : les fichiers ont été ajoutés au tableau de résultats, les fichiers ont été supprimés du tableau de résultats, des échantillons ont été ajoutés/ supprimés
Sample Type changed	Événements de quantification : 'Type d'échantillon' a été modifié
Std. Addition Actual concentration changed	—
Used column selection changed	Événements de quantification : 'Utiliser' a été modifié
Window/pane printed	Événements du projet : impression d'un document sur l'imprimante, impression du document terminée sur l'imprimante
Carte d'audit Page	
Project Audit Map changed	Événements du projet : Les paramètres du projet ont été modifiés
Project Audit Trail Printed	—
Project Audit Trail Exported	—
Espace de travail Batch	
Batch information imported from LIMS/ text	—
Print	Événements du projet : impression d'un document sur l'imprimante, impression du document terminée sur l'imprimante
Espace de travail Explorer	
Open Sample(s)	Événements du projet : le fichier de données a été ouvert
Recalibrate sample(s)	—
Recalibrate sample(s) started	—
Espace de travail LC Method	
Print	Événements du projet : impression d'un document sur l'imprimante, impression du document terminée sur l'imprimante
Espace de travail MS Method	

Événements d'audit

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

SCIEX OS ou CAC	Logiciel Analyst
Print	Événements du projet : impression d'un document sur l'imprimante, impression du document terminée sur l'imprimante
Espace de travail Queue	
Sample Transferred	—

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 la **Silent Audit Map**.

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

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

SCIEX OS ou CAC	Logiciel Analyst
Instrument Tune (SCIEX OS)	
Firmware changed	—
Manual Tuning	Événements de l'instrument : Les réglages des paramètres d'ajustement ont été modifiés
Automatic Tuning	Événements de l'instrument : Les réglages des paramètres d'ajustement ont été modifiés
Print Procedure Result in MS Tune	Événements du projet : impression d'un document sur l'imprimante, impression du document terminée sur l'imprimante
Hardware Configuration (SCIEX OS)	
Devices Activated	Événements de l'instrument : Le profil matériel a été activé
Devices Deactivated	Événements de l'instrument : Un profil matériel a été désactivé
Data File Checksum (SCIEX OS)	

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

SCIEX OS ou CAC	Logiciel Analyst
Wiff data file checksum has been changed	—
Espace de travail Explorer (SCIEX OS)	
Open Sample(s)	Événements du projet : le fichier de données a été ouvert
Recalibrate samples(s)	—
Recalibrate samples(s) started	—
Carte d'audit Page¹	
Workstation Audit Map changed	Événements de l'instrument : Les paramètres de l'instrument ont été modifiés
Workstation Audit Trail printed	—
Workstation Audit Trail exported	—
CAC Server (CAC)	
Project settings enabled/disabled in a workgroup	—
Project assigned/unassigned to a workgroup	—
User Role(s) assigned/unassigned to user(s) in workgroup	—
User(s)/UserGroup(s) assigned/unassigned to a workgroup	—
Workgroup added/deleted	—
Workgroup renamed	—
Workstation(s) assigned/unassigned to a workgroup	—
Espace de travail Queue (SCIEX OS)	
Sample moved in Queue	Événements de l'instrument : Échantillon passé de la position x à la position y de Batch File
Batch moved in Queue	Événements de l'instrument : Déplacer le lot
Requiring sample	Événements de l'instrument : Nouvelle acquisition d'un ou de plusieurs échantillons

¹ Ces événements sont enregistrés dans SCIEX OS et CAC.

Événements d'audit

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

SCIEX OS ou CAC	Logiciel Analyst
Sample starts to acquire	—
Print Queue	Événements du projet : impression d'un document sur l'imprimante, impression du document terminée sur l'imprimante
Sample acquisition has completed	Événements de l'instrument : Un échantillon a été ajouté à un fichier de données
Automatic reinjections Occurred	—
Automatic injection Occurred	—
Sécurité¹	
Auto logoff by system	Événements de l'instrument : Utilisateur déconnecté
Forced logoff by another user	Événements de l'instrument : Utilisateur déconnecté
Forced Logoff failed	—
Screen unlock failed	—
Secure Network Account credentials have been changed	Événements de l'instrument : Compte d'acquisition modifié
Secure Network Account credentials have been removed	Événements de l'instrument : Compte d'acquisition modifié
Secure Network Account credentials have been specified	Événements de l'instrument : Compte d'acquisition modifié
Security configuration changed	Événements de l'instrument : La configuration de la sécurité a été modifiée, Modification du verrouillage de l'écran, Modification de la déconnexion automatique
User added/deleted	Événements de l'instrument : Utilisateur ajouté, Utilisateur supprimé
User has logged in	Événements de l'instrument : Utilisateur connecté
User has logged out	Événements de l'instrument : Utilisateur déconnecté
User has turned off exclusive mode	—
User Login Failed	Événements de l'instrument : Échec de la connexion de l'utilisateur

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

SCIEX OS ou CAC	Logiciel Analyst
User management settings have been exported	—
User management settings have been imported	—
User management settings have been restored	—
User role assigned to user/user group	Événements de l'instrument : L'utilisateur a modifié le type d'utilisateur
User role deleted	Événements de l'instrument : Type d'utilisateur supprimé
User role modified	Événements de l'instrument : Type d'utilisateur modifié
UserLog ¹	
Print Event Log	—

Mappage d'autorisations entre SCIEX OS et le logiciel Analyst

C

Cette section est destinée aux utilisateurs qui migrent du logiciel Analyst vers SCIEX OS, afin de les aider à migrer leurs paramètres de sécurité. Elle présente les autorisations du logiciel Analyst qui correspondent aux autorisations de SCIEX OS.

Tableau C-1 : Mappage des autorisations

SCIEX OS	Logiciel Analyst
Espace de travail Batch	
Submit unlocked methods	—
Open	Lot : Ouvrir des lots existants
Save as	Lot : Créer de nouveaux lots, Importer, Éditer des lots, Sauvegarder des lots, Remplacer des lots
Submit	Lot : Soumettre des lots
Save	Lot : Sauvegarder des lots, Remplacer des lots
Save ion reference table	—
Add data sub-folders	—
Configure Decision Rules	—
Espace de travail Configuration	
General tab	—
General: change regional setting	—
General: full screen mode	—
General: Stop Windows services	—
LIMS Communication tab	—
Audit maps tab	Gestionnaire de registre d'audit : Modifier les paramètres de registre d'audit, Créer ou modifier des cartes d'audit
Queue tab	—
Queue: instrument idle time	—
Queue: max. number of acquired samples	—
Queue: other queue settings	—

Mappage d'autorisations entre SCIEX OS et le logiciel Analyst

Tableau C-1 : Mappage des autorisations (suite)

SCIEX OS	Logiciel Analyst
Projects tab	—
Projects: create project	Application Analyst : Créer un projet
Projects: apply an audit map template to an existing project	Gestionnaire de registre d'audit : Modifier les paramètres de registre d'audit
Projects: create root directory	Application Analyst : Créer un répertoire racine
Project: set current root directory	Application Analyst : Définir un répertoire racine
Projects: specify network credentials	—
Projects: Enable checksum writing for wiff data creation	—
Projects: clear root directory	—
Devices tab	Configuration du matériel : Créer, Supprimer, Éditer, Activer/Désactiver
User management tab	Config. de sécurité
Force user logoff	Application de déverrouillage/déconnexion
Espace de travail Event Log	
Access event log workspace	—
Archive log	—
Espace de travail Audit Trail	
Access audit trail workspace	Gestionnaire de registre d'audit : Consulter les données de registre d'audit
View active audit map	Gestionnaire de registre d'audit : Consulter les données de registre d'audit
Print/Export audit trail	Gestionnaire de registre d'audit : Consulter les données de registre d'audit
Volet Data Acquisition	
Start	—
Stop	—
Save	—
Espaces de travail MS Method et LC Method	
Access method workspace	—

Mappage d'autorisations entre SCIEX OS et le logiciel Analyst

Tableau C-1 : Mappage des autorisations (suite)

SCIEX OS	Logiciel Analyst
New	Méthode d'acquisition : Créer/Sauvegarder une méthode d'acquisition
Open	Méthode d'acquisition : Ouvrir une méthode d'acquisition en lecture seule (mode d'acquisition)
Save	Méthode d'acquisition : Remplacer des méthodes d'acquisition, Créer/Sauvegarder une méthode d'acquisition
Save as	Méthode d'acquisition : Remplacer des méthodes d'acquisition, Créer/Sauvegarder une méthode d'acquisition
Lock/Unlock method	—
Espace de travail Queue	
Manage	File d'attente d'échantillons : Acquérir à nouveau, Supprimer un échantillon ou lot, Déplacer un lot
Start/Stop	File d'attente d'échantillons : Lancer un échantillon, Arrêter un échantillon, Annuler un échantillon, Arrêter la file d'attente
Print	Éditeur de modèle rapports : Imprimer
Espace de travail Library	
Access library workspace	Explorer : Configurer l'emplacement de la bibliothèque, Configurer les options des utilisateurs de la bibliothèque, Ajouter l'enregistrement de la bibliothèque, Ajouter un spectre à la bibliothèque, Modifier l'enregistrement de la bibliothèque (remplace ajouter/supprimer si désactivé), Supprimer le spectre MS, Supprimer le spectre UV, Supprimer la structure, Afficher la bibliothèque, Rechercher dans la bibliothèque
CAC settings	
Enable Central Administration	—
Espace de travail MS Tune	
Access MS Tune workspace	—

Mappage d'autorisations entre SCIEX OS et le logiciel Analyst

Tableau C-1 : Mappage des autorisations (suite)

SCIEX OS	Logiciel Analyst
Advanced MS tuning	Régler : Optimisation des instruments, Réglage manuel, Éditer les options de réglage
Advanced troubleshooting	—
Quick status check	Régler : Opt instrument
Restore instrument data	Régler : Éditer les options de réglage, Éditer les données d'instrument
Espace de travail Explorer	
Access explorer workspace	—
Export	Explorer : Enregistrer les données en fichier texte
Print	Éditeur de modèle rapports : Imprimer
Options	—
Recalibrate	Régler : Étalonner à partir du spectre actuel
Espace de travail Analytics	
New results	Quantification : Créer de nouveaux tableaux de résultats
Create processing method	Quantification : Créer des méthodes de quantification
Modify processing method	Quantification : Modifier des méthodes existantes
Allow Export and Create Report of unlocked Results Table	—
Save results for Automation Batch	—
Change default quantitation method integration algorithm	Quantification : Modifier les options par défaut de la méthode
Change default quantitation method integration parameters	Quantification : Modifier les options par défaut de la méthode
Enable project modified peak warning	—
Add samples	Quantification : Ajouter et supprimer des échantillons dans le tableau de résultats
Remove selected samples	Quantification : Ajouter et supprimer des échantillons dans le tableau de résultats

Mappage d'autorisations entre SCIEX OS et le logiciel Analyst

Tableau C-1 : Mappage des autorisations (suite)

SCIEX OS	Logiciel Analyst
Export, import or remove external calibration	—
Modify sample name	Quantification : Modifier le nom d'un échantillon
Modify sample type	Quantification : Modifier le type d'échantillon
Modify sample ID	Quantification : Modifier l'ID d'un échantillon
Modify actual concentration	Quantification : Modifier la concentration en analyte
Modify dilution factor	Quantification : Modifier le facteur de dilution
Modify comments fields	Quantification : Modifier le commentaire d'un échantillon
Enable manual integration	Quantification : Intégrer manuellement
Set peak to not found	—
Include or exclude a peak from the results table	Quantification : Exclure les requêtes standard de l'étalonnage
Regression options	Quantification : Modifier les paramètres de régression
Modify the results table integration parameters for a single chromatogram	Quantification : Modifier des paramètres « simples » dans Peak Review, Modifier des paramètres « avancés » dans Peak Review
Modify quantitation method for results table component	Quantification : Modifier la méthode des tableaux de résultats
Create metric plot new settings	Quantification : Modifier ou créer des paramètres de tracés métriques
Add custom columns	Quantification : Créer ou modifier des colonnes de formules
Set peak review title format	—
Remove custom column	Quantification : Créer ou modifier des colonnes de formules
Results table display settings	Quantification : Modifier la précision des colonnes du tableau des résultats, Modifier la visibilité des colonnes du tableau des résultats, Modifier les paramètres du tableau des résultats
Lock results table	—

Mappage d'autorisations entre SCIEX OS et le logiciel Analyst

Tableau C-1 : Mappage des autorisations (suite)

SCIEX OS	Logiciel Analyst
Unlock results table	—
Mark results file as reviewed and save	—
Modify report template	Éditeur de modèle de rapports : Créer/ Modifier des modèles de rapports
Transfer results to LIMS	—
Modify barcode column	—
Change comparison sample assignment	—
Add the MSMS spectra to library	Explorer : Ajouter un spectre à un enregistrement dans la bibliothèque
Project default settings	Quantification : Modifier les paramètres généraux (par défaut)
Create report in all formats	—
Edit flagging criteria parameters	—
Automatic outlier removal parameter change	—
Enable automatic outlier removal	—
Update processing method via FF/LS	—
Update results via FF/LS	—
Enable grouping by adducts functionality	Quantification : Créer des groupes d'analytes, Modifier des groupes d'analytes
Browse for files	—
Enable standard addition	—
Set Manual Integration Percentage Rule	Quantification : Activer ou désactiver la règle de pourcentage dans Manual Integration

Somme de contrôle du fichier de données

D

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 pour le logiciel Analyst.

Activer ou désactiver la fonction Data File Checksum

1. Ouvrez l'espace de travail Configuration.
2. Cliquez sur **Projects**.
3. Si nécessaire, développez **Data File Security**.
4. Pour activer la fonction de somme de contrôle du fichier de données, cochez la case **Enable checksum writing for wiff data creation**. 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.

Adobe Acrobat Reader est nécessaire pour afficher ce document sous forme électronique. Pour télécharger la dernière version, accéder à <https://get.adobe.com/reader>.

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

Pour trouver la documentation du matériel, consulter le DVD de documentation du système ou du 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, contacter sciex.com/contact-us.
