
Software SCIEX OS

Guida del direttore del laboratorio



Questo documento viene fornito ai clienti che hanno acquistato apparecchiature SCIEX come guida all'utilizzo e al funzionamento delle stesse. Questo documento è protetto da copyright e qualsiasi riproduzione, parziale o totale, dei suoi contenuti è severamente vietata, a meno che SCIEX non abbia autorizzato per iscritto diversamente.

Il software menzionato in questo documento viene fornito con un contratto di licenza. La copia, le modifiche e la distribuzione del software con qualsiasi mezzo sono vietate dalla legge, salvo diversa indicazione contenuta nel contratto di licenza. Inoltre, il contratto di licenza può vietare che il software venga disassemblato, sottoposto a reverse engineering o decompilato per qualsiasi scopo. Le garanzie sono indicate in questo documento.

Alcune parti di questo documento possono far riferimento a produttori terzi e/o a loro prodotti, che possono contenere parti i cui nomi siano registrati come marchi e/o utilizzati come marchi dei rispettivi proprietari. Tali riferimenti mirano unicamente a designare i prodotti di terzi forniti da SCIEX e incorporati nelle sue apparecchiature e non implicano alcun diritto e/o licenza circa l'utilizzo o il permesso concesso a terzi di utilizzare i nomi di tali produttori e/o dei loro prodotti come marchi.

Le garanzie di SCIEX sono limitate alle garanzie esplicite fornite al momento della vendita o della licenza dei propri prodotti e costituiscono le uniche ed esclusive dichiarazioni, garanzie e obbligazioni di SCIEX. SCIEX non rilascia altre garanzie di nessun tipo, né espresse né implicite, comprese, a titolo di esempio, garanzie di commerciabilità o di idoneità per un particolare scopo, derivanti da leggi o altri atti normativi o dovute a pratiche e usi commerciali, tutte espressamente escluse, né si assume alcuna responsabilità o passività potenziale, compresi danni indiretti o conseguenti, per qualsiasi utilizzo da parte dell'acquirente o per eventuali circostanze avverse conseguenti.

Solo per scopi di ricerca. Non usare in procedure diagnostiche.

I marchi e/o i marchi registrati menzionati nel presente documento, inclusi i loghi associati, sono di proprietà di AB Sciex Pte. Ltd., o dei rispettivi proprietari, negli Stati Uniti e/o in altri Paesi (vedere: [sciex.com/trademarks](https://www.sciex.com/trademarks)).

AB Sciex™ è utilizzato su licenza.

© 2022 DH Tech. Dev. Pte. Ltd.



AB Sciex Pte. Ltd.

B1k33, #04-06 Marsiling Industrial Estate Road 3

Woodlands Central Industrial Estate, Singapore 739256

Sommario

Capitolo 1: Introduzione	6
Capitolo 2: Panoramica della configurazione di sicurezza	7
Sicurezza e conformità alle normative	7
Requisiti di sicurezza	7
Software SCIEX OS e sicurezza Windows: interazione	7
Audit trail in SCIEX OS e in Windows	8
Linee guida di sicurezza cliente: backup	8
21 CFR Parte 11	9
Configurazione di sistema	9
Configurazione di sicurezza di Windows	9
Utenti e gruppi	10
Supporto per Active Directory	10
File System Windows	10
Autorizzazioni file e cartelle	11
Controlli di sistema	11
Registri eventi	11
Avvisi di Windows	11
Capitolo 3: Licenze elettroniche	12
Prestito di una licenza elettronica basata su server	12
Restituzione di una licenza elettronica basata su server	13
Capitolo 4: Controllo dell'accesso	15
Posizione delle informazioni di sicurezza	15
Flusso di lavoro della sicurezza del software	15
Installazione di SCIEX OS	16
Requisiti di sistema	17
Opzioni di auditing preimpostate	17
Configurazione della modalità di protezione	17
Selezione della modalità di protezione	18
Configurazione delle opzioni di protezione della workstation (Mixed Mode)	18
Configurazione della notifica e-mail (Mixed Mode)	19
Configurazione dell'accesso a SCIEX OS	20
Autorizzazioni SCIEX OS	21
Informazioni su utenti e ruoli	29
Gestione utenti	40
Gestione dei ruoli	41
Esportazione e importazione di impostazioni di gestione utenti	42
Esportazione di impostazioni di gestione utenti	42
Ripristino delle impostazioni di gestione utenti	42

Sommario

Configurazione dell'accesso ai progetti e ai file di progetto	43
Cartelle del progetto	43
Tipi di file del software	43
Capitolo 5: Central Administrator Console	46
Utenti	46
Pool utenti	46
Ruoli utente e autorizzazioni	47
Gruppi di lavoro	58
Creazione di un gruppo di lavoro	59
Eliminazione di un gruppo di lavoro	59
Aggiunta di utenti o gruppi a un gruppo di lavoro	59
Aggiunta di workstation a un gruppo di lavoro	60
Aggiunta di progetti a un gruppo di lavoro	61
Gestione dei progetti	61
Informazioni su progetti e directory radice	62
Aggiunta di una directory radice	62
Eliminazione di una directory radice del progetto	63
Aggiunta di un progetto	63
Aggiunta di una sottocartella	63
Workstation	64
Aggiunta di una workstation	64
Eliminazione di una workstation	64
Report e funzionalità di sicurezza	65
Generazione di report di dati del gruppo di lavoro	65
Esportazione delle impostazioni software CAC	65
Importazione delle impostazioni software CAC	65
Ripristino delle impostazioni CAC	66
Capitolo 6: Acquisizione di rete	67
Informazioni sull'acquisizione di rete	67
Vantaggi che comporta l'uso dell'acquisizione di rete	67
Account di rete sicuro	67
Processo di trasferimento dei dati	68
Configurazione dell'acquisizione di rete	68
Specificare un account di rete sicura	69
Capitolo 7: Auditing	70
Audit trail	70
Mappe di audit	71
Configurazione delle mappe di audit	72
Modelli di mappe di audit installate	72
Utilizzo di mappe di audit	73
Mappe di audit di progetto	73
Mappe di audit della workstation	75
Visualizzazione, stampa e ricerca degli audit trail	77
Visualizzazione di un audit trail	77
Ricerca o filtro dei record di audit	77

Visualizzazione di un audit trail archiviato	78
Stampa di un audit trail	78
Esportazione di record degli audit trail	78
Record degli audit trail	79
Archivi degli audit trail	79
Appendice A: Accesso ai dati durante le interruzioni di rete	80
Visualizzazione ed elaborazione dati locale	80
Rimozione di campioni dalle cartelle di trasferimento in rete	80
Appendice B: Eventi di audit	82
Appendice C: Mapping di autorizzazioni tra SCIEX OS e il software Analyst	89
Appendice D: Data File Checksum	95
Abilitazione o disabilitazione dell'opzione Data File Checksum	95
Contatti	96
Formazione dei clienti	96
Centro di istruzione online	96
Assistenza SCIEX	96
Sicurezza informatica	96
Documentazione	96

Le informazioni contenute nel presente manuale sono destinate a due gruppi di destinatari:

- L'amministratore del laboratorio che si occupa, da un punto di vista funzionale, dell'uso quotidiano del software SCIEX OS e della strumentazione associata.
- L'amministratore di sistema che si occupa della protezione del sistema, nonché dell'integrità dello stesso e dei dati.

Panoramica della configurazione di sicurezza

2

Questa sezione spiega il modo in cui i componenti di auditing e controllo accessi del software SCIEX OS funzionano unitamente ai componenti di auditing e controllo accessi di Windows. Descrive inoltre come configurare la sicurezza di Windows prima di installare SCIEX OS.

Sicurezza e conformità alle normative

Il software SCIEX OS fornisce:

- Amministrazione personalizzabile per soddisfare i requisiti di ricerca e normativi.
- Strumenti di sicurezza e di audit a supporto della conformità con 21 CFR Parte 11 per l'uso della conservazione dei record elettronici.
- Gestione flessibile ed efficiente dell'accesso a funzioni critiche dello spettrometro di massa.
- Accesso controllato a dati e rapporti fondamentali.
- Facile gestione della protezione, unitamente alla protezione Windows.

Requisiti di sicurezza

I requisiti di sicurezza vanno da ambienti relativamente aperti, come laboratori di ricerca e accademici, ai laboratori più regolamentati, come i laboratori forensi.

Software SCIEX OS e sicurezza Windows: interazione

SCIEX OS e NTFS (Windows New Technology File System) dispongono di funzionalità di sicurezza progettate per controllare l'accesso ai dati e al sistema.

La sicurezza Windows garantisce il primo livello di protezione richiedendo agli utenti di accedere alla rete utilizzando un ID utente e una password univoci. Di conseguenza, solo gli utenti che vengono riconosciuti dalle impostazioni di sicurezza di rete o locali di Windows possono accedere al sistema. Per ulteriori informazioni, fare riferimento alla sezione: [Configurazione di sicurezza di Windows](#).

SCIEX OS Offre le modalità di accesso al sistema sicure seguenti:

- Mixed Mode
- Integrated Mode (impostazione predefinita)

Per ulteriori informazioni sulle modalità di sicurezza e sulle impostazioni di sicurezza, fare riferimento alla sezione: [Configurazione della modalità di protezione](#).

SCIEX OS fornisce inoltre ruoli completamente configurabili separati dai gruppi di utenti associati a Windows. Utilizzando i ruoli, il direttore di laboratorio può controllare l'accesso al

software e allo spettrometro di massa, funzione per funzione. Per ulteriori informazioni, fare riferimento alla sezione: [Configurazione dell'accesso a SCIEX OS](#).

Audit trail in SCIEX OS e in Windows

Le funzionalità di auditing del software SCIEX OS, insieme ai componenti di auditing di Windows integrati, sono fondamentali per la creazione e la gestione di record elettronici.

SCIEX OS fornisce un sistema di audit trail per soddisfare i requisiti della gestione di record elettronici. Registrazione separata degli audit trail:

- Modifiche alla tabella della calibrazione di massa o alla tabella di risoluzione, modifiche alla configurazione di sistema ed eventi di sicurezza.
- Eventi di creazione e modifica per progetti, tuning, lotti, dati, metodi di trattamento e file modello di report, nonché eventi di apertura, chiusura e stampa moduli. Gli eventi di eliminazione registrati nell'audit trail includono l'eliminazione di ruoli e di utenti in SCIEX OS.
- Creazione e modifica di informazioni sui campioni, parametri di integrazione picchi e metodo di elaborazione incorporato in una Results Table.

Nota: SCIEX OS non esegue l'auditing della creazione di metodi MS, metodi LC, lotti o metodi di elaborazione né delle modifiche apportate a essi. Questi file fungono da modelli. I valori dei parametri vengono letti da questi file al momento dell'acquisizione o dell'elaborazione e applicati all'attività. Per i metodi MS, i metodi LC e i lotti, i valori dei parametri vengono registrati nei file wiff e wiff2. Per i metodi di elaborazione, vengono registrati nel file qsession. Questi file fungono da record elettronici per queste informazioni.

Per un elenco completo di eventi di audit, fare riferimento alla sezione: [Eventi di audit](#).

SCIEX OS utilizza registro eventi dell'applicazione per acquisire informazioni sul funzionamento del software. Usare questo registro come supporto per la risoluzione dei problemi. Contiene informazioni dettagliate sullo spettrometro di massa, il dispositivo e le interazioni software.

In Windows sono contenuti registri eventi in cui vengono acquisiti eventi correlati alla sicurezza, al sistema e alle applicazioni. Nella maggior parte dei casi, l'auditing di Windows è concepito per catturare eventi eccezionali, quali problemi di connessione. L'amministratore può configurare questo sistema per catturare un'ampia gamma di eventi, come l'accesso a specifici file o attività di amministrazione di Windows. Per ulteriori informazioni, fare riferimento alla sezione: [Controlli di sistema](#).

Linee guida di sicurezza cliente: backup

Il backup dei dati cliente è responsabilità del cliente. Anche se il personale di supporto e assistenza SCIEX può fornire consigli e suggerimenti sul backup dei dati cliente, il cliente deve assicurarsi che il backup venga eseguito in conformità alle policy, alle esigenze e ai requisiti normativi. La frequenza e la copertura del backup dei dati clienti deve essere proporzionata ai requisiti organizzativi e alla criticità dei dati generati.

I clienti devono assicurarsi che i backup siano funzionali in quanto elementi fondamentali dalla gestione dati ed essenziali per il recupero in caso di attacco dannoso, guasto hardware o problema software. Non eseguire il backup del computer durante l'acquisizione dati o assicurarsi che i file in corso di acquisizione vengano ignorati dal software di backup. È vivamente consigliabile eseguire un backup completo del computer prima di installare qualsiasi aggiornamento della sicurezza o prima di eseguire qualsiasi riparazione sul computer. In questo modo sarà più semplice eseguire il rollback nel raro caso in cui una patch della sicurezza comprometta qualsiasi funzionalità dell'applicazione.

21 CFR Parte 11

SCIEX OS contiene i controlli tecnici per supportare le norme 21 CFR Part 11 con l'implementazione di:

- Sicurezza di Mixed Mode e Integrated Mode collegata alla sicurezza di Windows.
- Accesso controllato alla funzionalità mediante ruoli personalizzabili.
- Audit trail per il funzionamento dello strumento, l'acquisizione e la revisione dei dati, la generazione di rapporti.
- Firme elettroniche che usano una combinazione di ID utente e password.
- Configurazione adeguata del sistema operativo Windows.
- Procedure corrette e formazione adeguata in azienda.

SCIEX OS è progettato per essere usato nell'ambito di un sistema conforme alle norme 21 CFR Parte 11 e può essere configurato per supportare la conformità alla norma 21 CFR Parte 11. Il fatto che l'uso del software SCIEX OS sia conforme alle norme 21 CFR Parte 11 dipende dall'uso effettivo e dalla configurazione di SCIEX OS in laboratorio.

I servizi di convalida sono disponibili attraverso SCIEX Professional Services. Per maggiori informazioni, contattare complianceservices@sciex.com.

Nota: Non lasciare il software Instrument Parameters Converter su un sistema convalidato. È stato progettato per il trasferimento iniziale delle impostazioni strumento dal software Analyst a SCIEX OS. Assicurarsi di rimuovere il software Instrument Parameters Converter dal computer dopo l'uso.

Configurazione di sistema

La configurazione di sistema viene di solito effettuata dagli amministratori di rete o da utenti che dispongono di diritti di amministrazione locali o di rete.

Configurazione di sicurezza di Windows

Il sistema implementa le seguenti restrizioni per gli account utente Windows locali:

- La password di Windows deve essere modificata ogni 90 giorni.
- La password di Windows non può essere riutilizzata per almeno un'iterazione seguente. Non può essere uguale alla password precedente.

Panoramica della configurazione di sicurezza

- La password di Windows deve essere almeno otto caratteri.
- La password di Windows deve contenere almeno due dei seguenti quattro requisiti per soddisfare i requisiti di complessità:
 - Un carattere alfanumerico maiuscolo
 - Un carattere alfanumerico minuscolo
 - Un valore numerico
 - Un carattere speciale (ad esempio: ! @ # \$ % ^ &)
- Il nome utente Windows non può essere **admin**, **administrator** o **demo**.

L'amministratore del software SCIEX OS devono poter modificare le autorizzazioni file per la cartella SCIEX OS Data. Se questa cartella si trova in un computer locale, l'amministratore del software deve far parte del gruppo amministratori locali.

Per verificare che tutti gli utenti dispongano dell'accesso alle risorse per l'acquisizione di rete, l'amministratore di rete può definire un account di rete sicuro (SNA) nella risorsa di rete. Questo account deve disporre delle autorizzazioni di scrittura per le cartelle in rete che contengono la directory radice. È definito come SNA nelle proprietà per la directory radice.

Utenti e gruppi

SCIEX OS utilizza i nomi utente e le password registrati nel database di sicurezza del controller di dominio primario o Active Directory. Le password vengono gestite mediante gli strumenti messi a disposizione da Windows. Per ulteriori informazioni sull'aggiunta e la configurazione di utenti e ruoli, fare riferimento alla sezione: [Configurazione dell'accesso a SCIEX OS](#).

Supporto per Active Directory

Quando si aggiungono utenti nell'area di lavoro SCIEX OS Configuration, specificare gli account utente nel formato UPN (User Principal Name). Le seguenti versioni di Active Directory sono supportate:

- Server Windows 2012.
- Client Windows 7, 64 bit
- Client Windows 10, 64 bit

File System Windows

In SCIEX OS, i file e le directory devono essere archiviati in una partizione del disco rigido che utilizza il formato NTFS per controllare l'accesso ai file di SCIEX OS. Il file system FAT (File Allocation Table) non può controllare l'accesso a cartelle o file e pertanto, non è adatto per un ambiente sicuro.

Autorizzazioni file e cartelle

Per gestire la sicurezza, l'amministratore del software SCIEX OS deve disporre dei diritti per modificare le autorizzazioni per la cartella SCIEX OS Data. L'accesso deve essere configurato dall'amministratore di rete.

Nota: Considerare il livello di accesso di cui necessitano gli utenti per l'unità, la directory radice e la cartella dei progetti su ciascun computer. Configurare le autorizzazioni di condivisione e associate. Per maggiori informazioni sulla condivisione dei file, fare riferimento alla documentazione Windows.

Per informazioni sulle autorizzazioni cartella e file del software SCIEX OS, fare riferimento alla sezione: [Controllo dell'accesso](#).

Controlli di sistema

La funzione di controllo del sistema Windows può essere attivata al fine di rilevare violazioni della sicurezza o intrusioni nel sistema. Il controllo può essere impostato in modo da registrare diversi tipi di eventi correlati al sistema. Ad esempio, la funzione di auditing può essere attivata per la registrazione di tutti i tentativi di accesso al sistema riusciti o meno nel registro eventi.

Registri eventi

Il visualizzatore eventi di Windows registra gli eventi controllati nel registro di sicurezza, nel registro di sistema o nel registro dell'applicazione.

Personalizzare i registri eventi come descritto di seguito:

- Configurare un registro eventi di dimensioni appropriate.
- Impostare la sovrascrittura automatica degli eventi precedenti.
- Eseguire le impostazioni di sicurezza del computer Windows.

Può essere implementato un processo di controllo e archiviazione. Per ulteriori informazioni sulle impostazioni di sicurezza e sui criteri di audit, fare riferimento alla documentazione di Windows.

Avvisi di Windows

Se si verifica un problema che interessa il sistema o l'utente, configurare la rete in modo da inviare un messaggio automatico a una persona designata, ad esempio l'amministratore di sistema, sullo stesso o su un altro computer.

- Su entrambi i computer di invio e ricezione, avviare il servizio Messenger nel pannello di controllo Windows Services.
- Sul computer di invio, avviare il servizio Alert nel pannello di controllo Windows Services.

Per ulteriori informazioni sulla creazione di un oggetto avviso, fare riferimento alla documentazione di Windows.

Per SCIEX OS, le licenze elettroniche possono essere vincolate al nodo o basate su server. Per il software Central Administrator Console (CAC), le licenze elettroniche possono essere solo vincolate al nodo.

L'ID attivazione potrebbe essere richiesto per le chiamate all'assistenza future. Per accedere all'ID attivazione della licenza basata su server o vincolata al nodo:

- Nell'area di lavoro Configuration fare clic su **Licenses** nella finestra del software SCIEX OS.

Nota: Assicurarsi di effettuare il rinnovo della licenza prima della scadenza.

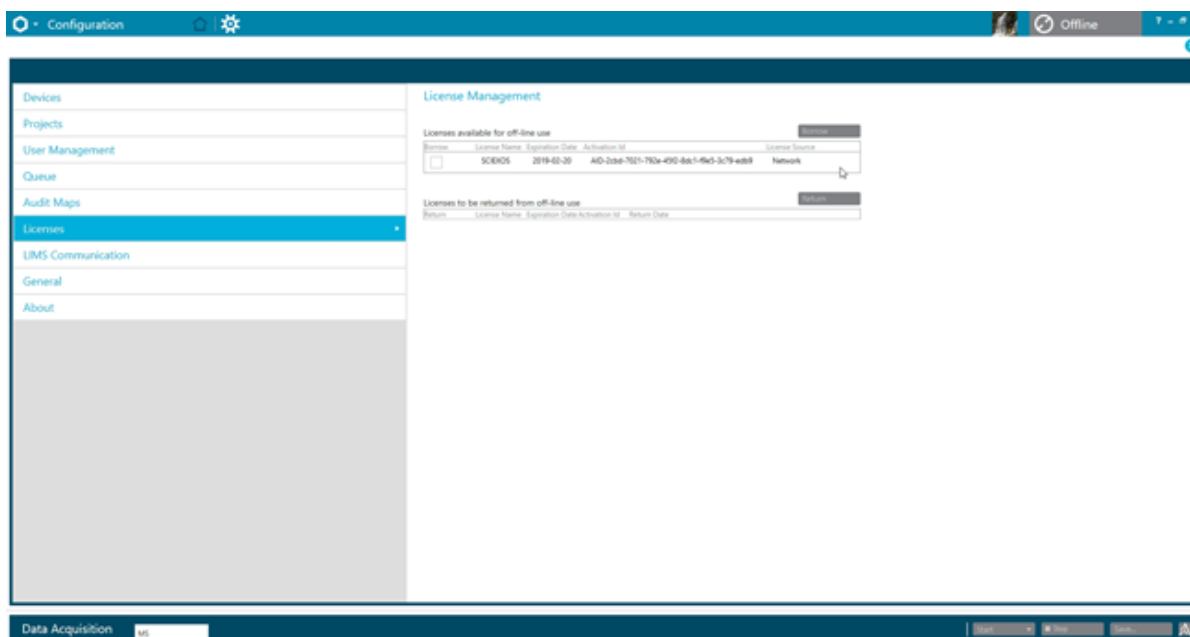
Prestito di una licenza elettronica basata su server

È necessario disporre di una licenza per utilizzare il software SCIEX OS. Se sono in uso licenze basate su server, gli utenti che desiderano lavorare offline possono prenotare una licenza per un massimo di 7 giorni. Durante questo periodo, la licenza elettronica presa in prestito può essere usata su un computer specifico.

Nota: Questa procedura non è applicabile al software Central Administrator Console (CAC).

1. Aprire l'area di lavoro Configuration.
2. Fare clic su **Licenses**.
La tabella Licenses available for off-line use mostra tutte le licenze disponibili per il prestito.

Figura 3-1: Gestione delle licenze: prestito di una licenza



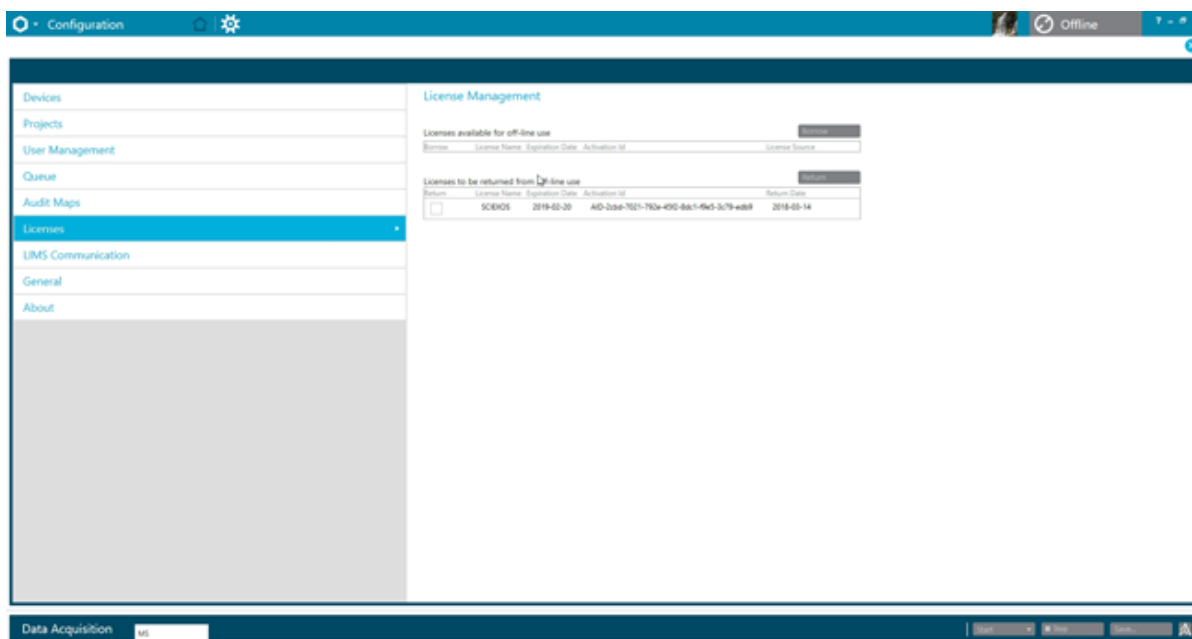
3. Selezionare la licenza da prendere in prestito e fare clic su **Borrow**.

Restituzione di una licenza elettronica basata su server

Nota: Questa procedura non è applicabile al software Central Administrator Console (CAC).

1. Aprire l'area di lavoro Configuration.
2. Fare clic su **Licenses**.
La tabella Licenses to be returned from off-line use mostra tutte le licenze idonee alla restituzione, ovvero tutte le licenze prese in prestito dal computer in uso.

Figura 3-2: Gestione delle licenze: restituzione di una licenza



3. Selezionare le licenze da restituire e fare clic su **Return**.

In questa sezione viene descritto come controllare l'accesso a SCIEX OS. Per controllare l'accesso al software SCIEX OS, l'amministratore esegue le seguenti operazioni:

Nota: per eseguire le attività in questa sezione, l'utente deve disporre dei privilegi di amministratore locale per la workstation su cui il software viene installato.

- Installare e configurare SCIEX OS.
- Aggiungere ed eliminare utenti e ruoli.
- Configurare l'accesso ai progetti e file di progetto nella directory radice.

Questa procedura fornisce istruzioni per l'amministrazione locale di SCIEX OS. Per l'amministrazione centralizzata di SCIEX OS, fare riferimento alla sezione: [Central Administrator Console](#)

Nota: Eventuali modifiche alla configurazione di SCIEX OS diventeranno effettive al riavvio del software SCIEX OS.

Posizione delle informazioni di sicurezza

Tutte le informazioni di sicurezza sono archiviate sul computer locale, nella cartella `C:\ProgramData\SCIEX\Clearcore2.Acquisition` in un file denominato `Security.data`.

Flusso di lavoro della sicurezza del software

SCIEX OS interagisce con i componenti di auditing degli eventi di sicurezza, applicazioni e sistema degli strumenti amministrativi di Windows.

Configurazione della protezione ai seguenti livelli:

- Autenticazione Windows: accesso al computer.
- Autenticazione Windows: accesso a file e cartelle.
- Autenticazione SCIEX OS: possibilità di aprire SCIEX OS.
- Autorizzazione SCIEX OS: accesso alle funzionalità in SCIEX OS.

Per l'elenco di attività per la configurazione della sicurezza, fare riferimento alla tabella: [Tabella 4-1](#). Per le opzioni di impostazione dei vari livelli di sicurezza, fare riferimento alla tabella: [Tabella 4-2](#).

Tabella 4-1: Flusso di lavoro per la configurazione della sicurezza

Attività	Procedura
Installare SCIEX OS.	Fare riferimento al documento: <i>Guida all'installazione del software SCIEX OS</i> .
Configurare l'accesso a SCIEX OS.	Fare riferimento alla sezione: Configurazione dell'accesso a SCIEX OS .
Configurare Windows File Security e NTFS.	Fare riferimento alla sezione: Configurazione dell'accesso ai progetti e ai file di progetto .

Tabella 4-2: Opzioni per la configurazione di sicurezza

Opzione	CFR 21 Parte 11
Sicurezza di Windows	
Configurare utenti e gruppi (autenticazione).	Sì
Abilitare l'auditing di Windows e di file e directory.	Sì
Impostare le autorizzazioni file (autorizzazione).	Sì
Installazione di SCIEX OS	
Installare SCIEX OS.	Sì
Aprire il Visualizzatore eventi per ispezionare l'installazione.	Sì
Sicurezza del software	
Selezionare la modalità di sicurezza.	Sì
Configurare gli utenti e i ruoli di SCIEX OS.	Sì
Configurare la notifica e-mail.	Sì
Creare modelli di mappe di audit e configurare le mappe di audit trail del progetto e della workstation.	Sì
Abilitare la funzione di checksum per i file wiff.	Sì
Common Tasks	
Aggiungere nuovi progetti.	Sì

Installazione di SCIEX OS

Prima di installare SCIEX OS, leggere questi documenti disponibili nel DVD di installazione del software o nel pacchetto di download Web: *Guida all'installazione del software* e *Note di rilascio*. Prima di completare la sequenza di installazione, assicurarsi di comprendere la differenza tra un computer di elaborazione e un computer di acquisizione.

Requisiti di sistema

Per i requisiti di installazione minimi, fare riferimento al documento: *Guida all'installazione del software*.

Opzioni di auditing preimpostate

Per una descrizione delle mappe di audit installate, fare riferimento alla sezione: [Modelli di mappe di audit installate](#). Dopo l'installazione, l'amministratore del software SCIEX OS può creare mappe personalizzate e assegnare un'altra audit map nell'area di lavoro Configuration.

Configurazione della modalità di protezione

Questa sezione descrive le opzioni Security Mode che si trovano nella pagina User Management nell'area di lavoro Configuration.

Integrated Mode: se l'utente attualmente connesso a Windows viene identificato come utente nel software, quell'utente ha accesso a SCIEX OS.

Integrated Mode: se l'utente attualmente connesso a Windows viene identificato come utente nel software, quell'utente ha accesso a .

Mixed Mode: gli utenti accedono separatamente a Windows e al software. Le credenziali utilizzate per accedere a Windows non possono essere le stesse credenziali utilizzate per accedere a . Utilizzare questa modalità per consentire a un gruppo di utenti di accedere a Windows con lo stesso set di credenziali, ma richiedere a ogni utente di accedere al software con credenziali univoche. Queste credenziali univoche possono essere assegnate a un ruolo specifico, come in modalità Integrated.

Se si seleziona la modalità Mixed, sono disponibili le opzioni Screen Lock e Auto Logoff.

Screen Lock e Auto Logoff: per motivi di sicurezza, è possibile impostare il blocco dello schermo del computer dopo un determinato periodo di inattività. È anche possibile impostare un timer di disconnessione automatica in modo che il software si chiuda dopo essere stato bloccato per un periodo di tempo definito. Le opzioni Screen Lock e Auto Logoff sono disponibili solo nella modalità Mixed.

Nota: Quando lo schermo si blocca, acquisizione ed elaborazione continuano. La disconnessione automatica non viene effettuata se è in corso l'elaborazione o se la Results Table non è stata salvata. Quando l'utente viene disconnesso in modo forzato, ogni elaborazione si interrompe e tutti i dati non salvati vanno persi. L'acquisizione continua dopo la disconnessione dell'utente, sia automatica che manuale.

Security Notification: il software può essere configurato per inviare automaticamente una notifica e-mail dopo un numero configurabile di errori di accesso entro un periodo di tempo configurabile, per avvisare dei tentativi di accesso al sistema da parte di utenti non autorizzati. Il numero di errori di accesso può variare da 3 a 7 e il periodo da 5 minuti a 24 ore.

Nota: Per i gruppi di lavoro amministrati dal software Central Administrator Console (CAC), la modalità di sicurezza non può essere gestita con SCIEX OS.

Selezione della modalità di protezione

1. Aprire l'area di lavoro Configuration.
2. Fare clic su **User Management**.
3. Fare clic sulla scheda **Security Mode**.
4. Selezionare **Integrated Mode** o **Mixed Mode**. Fare riferimento alla sezione: [Configurazione della modalità di protezione](#).
5. Fare clic su **Save**.
Viene visualizzata una finestra di dialogo di conferma.
6. Fare clic su **OK**.

Configurazione delle opzioni di protezione della workstation (Mixed Mode)

Procedure preliminari
<ul style="list-style-type: none">• Impostare la modalità di protezione su Mixed Mode. Fare riferimento alla sezione: Configurazione della modalità di protezione.

Se si seleziona Mixed Mode, sono disponibili le opzioni Screen Lock e Auto Logoff.

1. Aprire l'area di lavoro Configuration.
2. Fare clic su **User Management**.
3. Aprire la scheda Security Mode.
4. Per configurare la funzione Screen Lock, attenersi alla procedura seguente:
 - a. Selezionare **Screen Lock**.
 - b. Nel campo **Wait**, specificare un periodo di tempo in minuti.
Se la workstation resta inattiva per questo periodo di tempo, viene automaticamente bloccata. L'utente connesso può sbloccare la workstation inserendo le credenziali corrette, oppure l'amministratore può disconnettere l'utente.
5. Per configurare la funzione Auto Logoff, attenersi alla procedura seguente:
 - a. Selezionare **Auto Logoff**.
 - b. Nel campo **Wait**, specificare un periodo di tempo in minuti. Se la workstation resta bloccata per questo periodo di tempo, sia che sia stata bloccata automaticamente o manualmente, l'utente attualmente connesso viene disconnesso. Ogni elaborazione si interrompe. L'acquisizione, tuttavia, continua.
6. Fare clic su **Save**.
Viene visualizzata una finestra di dialogo di conferma.

7. Fare clic su **OK**.

Configurazione della notifica e-mail (Mixed Mode)

Procedure preliminari

- Impostare la modalità di protezione su Mixed Mode. Fare riferimento alla sezione: [Configurazione della modalità di protezione](#).

Il software può essere configurato per inviare un messaggio e-mail dopo un numero configurabile di errori di accesso entro un periodo configurabile. Il numero di errori di accesso può variare da 3 a 7 e il periodo da 5 minuti a 24 ore.

Il computer su cui è installato il software deve poter comunicare con un server SMTP con una porta aperta.

1. Aprire l'area di lavoro Configuration.
2. Fare clic su **User Management**.
3. Aprire la scheda Security Mode.
4. Selezionare la casella di controllo **Send e-mail messages after** e quindi specificare quanti errori di accesso entro quale periodo, in minuti, genereranno una notifica e-mail.

Suggerimento! Per disabilitare la notifica, deselezionare la casella di controllo **Send e-mail messages after**.

5. Nel campo **SMTP Server**, digitare il nome del server SMTP.

Nota: L'account SMTP invia le e-mail al server e-mail. Il server SMTP è definito nell'applicazione e-mail aziendale.

6. Nel campo **Port Number**, digitare il numero della porta aperta.
Fare clic su **Apply Default** per inserire il numero di porta predefinito, 25.
7. Nel campo **To**, digitare l'indirizzo e-mail a cui verrà inviato il messaggio. Ad esempio: nomeutente@dominio.com.
8. Nel campo **From**, digitare l'indirizzo e-mail che comparirà nel campo **From** del messaggio.
9. Nel campo **Subject**, digitare l'oggetto del messaggio.
10. Nel campo **Message**, digitare il testo che verrà incluso nel corpo del messaggio.
11. Fare clic su **Save**.
Viene visualizzata una finestra di dialogo di conferma.
12. Fare clic su **OK**.
13. Per controllare la configurazione, fare clic su **Send Test Mail**.

Configurazione dell'accesso a SCIEX OS

Prima di configurare la sicurezza, procedere come segue:

- Eliminare tutti gli utenti e i gruppi utente non necessari, ad esempio replicatore, power user e operatore di backup, dal computer locale e dalla rete.

Nota: Ogni computer SCIEX è configurato con un account di amministratore locale, **abservice**. Questo account viene utilizzato dall'assistenza SCIEX e dal supporto tecnico per installare, riparare e supportare il sistema. Non rimuovere né disattivare questo account. Se l'account deve essere rimosso o disattivato, preparare un piano alternativo per l'accesso SCIEX e comunicarlo all'FSE locale.

- Aggiungere gruppi utente contenenti gruppi a cui saranno assegnate attività non amministrative.
- Configurare le autorizzazioni di sistema.
- Creare procedure e criteri account idonei per gli utenti in Criteri gruppo

Fare riferimento alla documentazione di Windows per ulteriori informazioni su:

- Utenti e gruppi e utenti Active Directory.
- Criteri di blocco password e account per gli account utente.
- Criteri diritti utente.

Quando gli utenti lavorano in un ambiente Active Directory, le impostazioni dei criteri gruppo di Active Directory influiscono sulla sicurezza del computer. Discutere i criteri gruppo con l'amministratore Active Directory come parte di una distribuzione completa del software SCIEX OS.

Autorizzazioni SCIEX OS

Figura 4-1: Pagina User Management

The screenshot shows the 'User Management' page in the SCIEX OS interface. The left sidebar contains navigation options: Devices, Projects, User Management (selected), Queue, Audit Maps, Licenses, LIMS Communication, General, and About. The main content area is titled 'User Roles and Permission Categories' and displays a table of permissions for four roles: Administrator, Method Developer, Analyst, and Reviewer.

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"/>

Tabella 4-3: Autorizzazioni

Autorizzazione	Descrizione
Batch (Lotto)	
Submit unlocked methods	(Invia metodi sbloccati) Consente agli utenti di inviare lotti contenenti metodi sbloccati.
Open	(Apri) Consente agli utenti di aprire lotti esistenti.
Save as	(Salva con nome) Consente agli utenti di salvare lotti con un nuovo nome.
Submit	(Invia) Consente agli utenti di inviare lotti.
Save	(Salva) Consente agli utenti di salvare un lotto, sovrascrivendo il contenuto esistente.
Save ion reference table	(Salva tabella di riferimento ionica) Consente agli utenti di modificare la tabella di riferimento ionica.

Tabella 4-3: Autorizzazioni (continua)

Autorizzazione	Descrizione
Add data sub-folders	(Aggiungi sottocartelle dati) Consente agli utenti di creare sottocartelle per archiviare dati.
Configure Decision Rules	(Configura regole di decisione) Consente agli utenti di aggiungere e modificare regole di decisione.
Configuration (Configurazione)	
General tab	(Scheda Generale) Consente agli utenti di aprire la pagina Generale nell'area di lavoro Configuration.
General: change regional setting	(Generale: modifica impostazioni regionali) Consente agli utenti di applicare le impostazioni internazionali di sistema correnti a SCIEX OS.
General: full screen mode	(Generale: modalità schermo intero) Consente agli utenti di abilitare e disabilitare la modalità schermo intero.
General: Stop Windows services	(Generale: arresta i servizi di Windows) Consente agli utenti di abilitare o disabilitare l'opzione Windows Settings .
LIMS communication tab	(Scheda di comunicazione LIMS) Consente agli utenti di aprire la pagina LIMS Communication nell'area di lavoro Configuration.
Audit maps tab	(Scheda Mappe di audit) Consente agli utenti di aprire la pagina Audit Maps nell'area di lavoro Configuration.
Queue tab	(Scheda Coda) Consente agli utenti di aprire la pagina Queue nell'area di lavoro Configuration.
Queue: instrument idle time	(Coda: tempo inattività strumento) Consente agli utenti di impostare il tempo di inattività dello strumento.
Queue: max number of acquired samples	(Coda: numero max di campioni acquisiti) Consente agli utenti di impostare il numero massimo di campioni acquisiti consentito.
Queue: other queue settings	(Coda: altre impostazioni coda) Consente agli utenti di configurare altre impostazioni coda.
Projects tab	(Scheda Progetti) Consente agli utenti di aprire la pagina Projects nell'area di lavoro Configuration.
Projects: create project	(Progetti: crea progetto) Consente agli utenti di creare progetti.
Projects: apply an audit map template to an existing project	(Progetti: applica un modello di mappa di audit a un progetto esistente) Consente agli utenti di applicare una mappa di audit a un progetto.
Projects: create root directory	(Progetti: crea directory radice) Consente agli utenti di creare una directory radice in cui archiviare progetti.

Tabella 4-3: Autorizzazioni (continua)

Autorizzazione	Descrizione
Projects: set current root directory	(Progetti: imposta directory radice corrente) Consente agli utenti di modificare la directory radice per un progetto.
Projects: specify network credentials	(Progetti: specifica credenziali di rete) Consente agli utenti di specificare un account di rete sicuro (SNA) da utilizzare durante l'acquisizione di rete se l'utente connesso non ha accesso alla risorsa di rete.
Projects: Enable checksum writing for wiff data creation	(Progetti: consenti scrittura del checksum per la creazione di dati wiff) Consente agli utenti di configurare il software per la scrittura di checksum in file di dati wiff.
Projects: clear root directory	(Progetti: cancella directory radice) Consente agli utenti di eliminare una directory radice dall'elenco.
Devices tab	(Scheda Dispositivi) Consente agli utenti di aprire la pagina Devices nell'area di lavoro Configuration.
User management tab	(Scheda Gestione utenti) Consente agli utenti di aprire la pagina User Management nell'area di lavoro Configuration.
Force user logoff	(Impone disconnessione utente) Consente agli utenti di imporre la disconnessione di un utente attualmente connesso a SCIEX OS. Consente agli utenti di imporre la disconnessione di un utente attualmente connesso al software SCIEX OS.
Event Log (Registro eventi)	
Access event log workspace	(Accedi all'area di lavoro log eventi) Consente agli utenti di aprire l'area di lavoro Event Log.
Archive log	(Archivia log) Consente agli utenti di archiviare il log eventi.
Audit Trail (Audit Trail)	
Access audit trail workspace	(Accedi all'area di lavoro audit trail) Consente agli utenti di aprire l'area di lavoro Audit Trail.
View active audit map	(Visualizza mappa di audit attiva) Consente agli utenti di visualizzare la mappa di audit attiva per una workstation o un progetto nell'area di lavoro Audit Trail.
Print/Export audit trail	(Stampa/Esporta audit trail) Consente agli utenti di stampare o esportare l'audit trail.
CAC Server (Server CAC) (solo CAC)	
Manage Workgroups	(Gestisci gruppi di lavoro) Consente agli utenti di creare e gestire gruppi di lavoro nell'area di lavoro User Management.

Tabella 4-3: Autorizzazioni (continua)

Autorizzazione	Descrizione
Manage Workgroups Projects	(Gestisci progetti di gruppi di lavoro) Consente agli utenti di creare e gestire progetti di gruppi di lavoro nell'area di lavoro User Management.
Data Acquisition Panel (Pannello di acquisizione dati)	
Start	(Avvia) Consente agli utenti di avviare l'acquisizione nel riquadro Data Acquisition.
Stop	(Arresta) Consente agli utenti di arrestare l'acquisizione nel riquadro Data Acquisition.
Save	(Salva) Consente agli utenti di salvare i dati acquisiti con un nome file diverso nel riquadro Data Acquisition.
MS & LC Method (Metodo MS e LC)	
Access method workspace	(Accedi all'area di lavoro metodo) Consente agli utenti di aprire le aree di lavoro MS Method e LC Method.
New	(Nuovo) Consente agli utenti di creare metodi MS e LC.
Open	(Apri) Consente agli utenti di aprire i metodi MS e LC.
Save	(Salva) Consente agli utenti di salvare un metodo, sovrascrivendo il contenuto esistente.
Save as	(Salva con nome) Consente agli utenti di salvare metodi con un nuovo nome.
Lock/Unlock method	(Blocca/Sblocca metodo) Consente agli utenti di bloccare metodi, di impedirne la modifica e di sbloccarli.
Queue (Coda)	
Manage	(Gestisci) Consente agli utenti di aprire l'area di lavoro Queue.
Start/Stop	(Avvia/Arresta) Consente agli utenti di avviare o arrestare la coda.
Print	(Stampa) Consente agli utenti di stampare la coda.
Library (Libreria)	
Access library workspace	(Accedi all'area di lavoro Libreria) Consente agli utenti di aprire l'area di lavoro Library. Non applicabile al flusso di lavoro di quantificazione.
CAC settings (Client CAC)	
Enable Central Administration	(Abilita amministrazione centrale) Consente agli utenti di configurare SCIEX OS per l'amministrazione centrale con il software Central Administrator Console (CAC).

Tabella 4-3: Autorizzazioni (continua)

Autorizzazione	Descrizione
MS Tune (Tuning MS)	
Access MS Tune workspace	(Accedi all'area di lavoro MS Tune) Consente agli utenti di aprire l'area di lavoro MS Tune.
Advanced MS tuning	(Tuning MS avanzato) (Sistemi X500 QTOF) Consente agli utenti di accedere alle opzioni di tuning avanzato, tra cui Detector Optimization, Positive and Negative Q1 Unit Tuning, Positive and Negative TOF MS Tuning e Positive and Negative Q1 High Tuning.
Advanced troubleshooting	(Risoluzione dei problemi avanzata) Consente agli utenti di aprire la finestra di dialogo Advanced Troubleshooting.
Quick status check	(Controllo rapido stato) (Sistemi X500 QTOF) Consente agli utenti di eseguire i controlli Positive and Negative Quick Status Checks.
Restore instrument data	(Ripristina dati strumento) Consente agli utenti di ripristinare le impostazioni di tuning salvate in precedenza.
Explorer (Esplora)	
Access Explorer workspace	(Accedi all'area di lavoro Esplora) Consente agli utenti di aprire l'area di lavoro Explorer.
Export	(Esporta) Consente agli utenti di esportare dati dall'area di lavoro Explorer.
Print	(Stampa) Consente agli utenti di stampare dati nell'area di lavoro Explorer.
Options	(Opzioni) Consente agli utenti di modificare le opzioni per l'area di lavoro Explorer.
Recalibrate	(Ricalibra) Consente agli utenti di ricalibrare campioni e spettri nell'area di lavoro Explorer. Non applicabile al flusso di lavoro di quantificazione.
Analytics (Analisi)	
New results	(Nuovi risultati) Consente agli utenti di creare Results Table.
Create processing method	(Crea metodo di trattamento) Consente agli utenti di creare metodi di trattamento.
Modify processing method	(Modifica metodo di trattamento) Consente agli utenti di modificare i metodi di trattamento.
Allow Export and Create Report of unlocked Results Table	(Consenti esportazione e crea report della Results Table sbloccata) Consente agli utenti di esportare o generare un report da una Results Table o da una tabella delle statistiche, se la Results Table non è bloccata.

Tabella 4-3: Autorizzazioni (continua)

Autorizzazione	Descrizione
Save results for Automation Batch	(Salva risultati per lotto automazione) Consente di salvare le Results Table create automaticamente nell'area di lavoro Batch. Questa autorizzazione è necessaria per l'elaborazione automatica durante l'acquisizione.
Change default quantitation method integration algorithm	(Modifica l'algoritmo di integrazione metodo di quantificazione predefinito) Consente agli utenti di modificare l'algoritmo di integrazione nelle impostazioni predefinite del progetto.
Change default quantitation method integration parameters	(Modifica i parametri di integrazione metodo di quantificazione predefinito) Consente agli utenti di modificare i parametri di integrazione nelle impostazioni predefinite del progetto.
Enable project modified peak warning	(Attiva avviso picco modificato progetto) Consente agli utenti di attivare la proprietà avviso picco modificato per un progetto.
Add samples	(Aggiungi campioni) Consente agli utenti di aggiungere campioni a una Results Table.
Remove selected samples	(Rimuovi campioni selezionati) Consente agli utenti di rimuovere campioni da una Results Table.
Export, import, or remove external calibration	(Esporta, importa o rimuovi calibrazione esterna) Consente agli utenti di esportare, importare o rimuovere calibrazioni esterne.
Modify sample name	(Modifica nome campione) Consente agli utenti di modificare il nome del campione nella Results Table.
Modify sample type	(Modifica tipo di campione) Consente agli utenti di modificare il tipo di campione, ad esempio standard, quality control (QC) o unknown nella Results Table.
Modify sample ID	(Modifica ID campione) Consente agli utenti di modificare l'ID campione nella Results Table.
Modify actual concentration	(Modifica concentrazione effettiva) Consente agli utenti di modificare la concentrazione effettiva dei campioni standard e QC nella Results Table.
Modify dilution factor	(Modifica fattore di diluizione) Consente agli utenti di modificare il fattore di diluizione nella Results Table.

Tabella 4-3: Autorizzazioni (continua)

Autorizzazione	Descrizione
Modify comment fields	(Modifica campi commenti) Consente agli utenti di modificare i campi dei commenti: <ul style="list-style-type: none"> • Component Comment • IS Comment • IS Peak Comment • Peak Comment • Sample Comment
Enable manual integration	(Abilita integrazione manuale) Consente agli utenti di eseguire l'integrazione manuale.
Set peak to Not Found	(Imposta picco su Non trovato) Consente agli utenti di impostare un picco su Not Found .
Include or exclude a peak from the Results Table	(Includi o escludi un picco dalla Results Table) Consente agli utenti di includere ed escludere picchi dalla Results Table.
Regression options	(Opzioni regressione) Consente agli utenti di modificare le opzioni di regressione nel riquadro Calibration Curve.
Modify Results Table integration parameters for a single chromatogram	(Modifica parametri di integrazione results table per un singolo cromatogramma) Consente agli utenti di modificare i parametri di integrazione per un singolo cromatogramma nel riquadro Peak Review.
Modify quantitation method for the Results Table component	(Modifica metodo di quantificazione per il componente Results Table) Consente agli utenti di selezionare un metodo di trattamento diverso per un componente nel riquadro Peak Review con l'opzione Update Processing Method for Component .
Create metric plot new settings	(Crea nuove impostazioni tracciato metrico) Consente agli utenti di creare nuovi tracciati metrici e modificare le impostazioni.
Add custom columns	(Aggiungi colonne personalizzate) Consente agli utenti di aggiungere colonne personalizzate a una Results Table.
Set peak review title format	(Imposta formato titolo revisione picco) Consente agli utenti di modificare il titolo revisione picco.
Remove custom column	(Rimuovi colonna personalizzata) Consente agli utenti di rimuovere colonne personalizzate da una Results Table.
Results Table display settings	(Impostazioni di visualizzazione Results Table) Consente agli utenti di personalizzare le colonne mostrate nella Results Table.

Tabella 4-3: Autorizzazioni (continua)

Autorizzazione	Descrizione
Lock Results Table	(Blocca Results Table) Consente agli utenti di bloccare una Results Table per impedire la modifica.
Unlock Results Table	(Sblocca Results Table) Consente agli utenti di sbloccare una Results Table per consentire la modifica.
Mark Results file as reviewed and save	(Contrassegna il file dei risultati come rivisto e salvato) Consente agli utenti di contrassegnare una Results Table come rivista e salvata.
Modify report template	(Modifica modello di report) Consente agli utenti di modificare i modelli di report.
Transfer results to LIMS	(Trasferisci risultati a LIMS) Consente agli utenti di caricare risultati in un sistema LIMS (Laboratory Information Management System).
Modify barcode column	(Modifica colonna codice a barre) Consente agli utenti di modificare la colonna Barcode in una Results Table.
Change comparison sample assignment	(Modifica assegnazione campione di confronto) Consente agli utenti di modificare il campione di confronto specificato nella colonna Comparison della Results Table.
Add the MSMS spectra to library	(Aggiungi gli spettri MSMS alla libreria) Consente agli utenti di aggiungere gli spettri MS/MS selezionati a una libreria. Non applicabile al flusso di lavoro di quantificazione.
Project default settings	(Impostazioni predefinite progetto) Consente agli utenti di modificare le impostazioni di elaborazione qualitativa e quantitativa predefinite del progetto.
Create report in all formats	(Crea report in tutti i formati) Consente agli utenti di generare report in tutti i formati. Gli utenti che non hanno questa autorizzazione possono generare solo report in formato PDF.
Edit flagging criteria parameters	(Modifica parametri criteri di segnalazione) Consente agli utenti di modificare i parametri di segnalazione in un metodo di trattamento.
Automatic outlier removal parameter change	(Modifica automatica parametro di rimozione anomalia) Consente agli utenti di modificare i parametri per la rimozione automatica delle anomalie.
Enable automatic outlier removal	(Abilita rimozione automatica anomalie) Consente agli utenti di modificare il metodo di trattamento per attivare la funzionalità di rimozione automatica delle anomalie.

Tabella 4-3: Autorizzazioni (continua)

Autorizzazione	Descrizione
Update processing method via FF/LS	(Aggiorna metodo di trattamento tramite FF/LS) Consente agli utenti di aggiornare i metodi di trattamento mediante Formula Finder e Library Search. Non applicabile al flusso di lavoro di quantificazione.
Update results via FF/LS	(Aggiorna risultati tramite FF/LS) Consente agli utenti di aggiornare i risultati mediante Formula Finder e Library Search. Non applicabile al flusso di lavoro di quantificazione.
Enable grouping by adducts functionality	(Abilita raggruppamento per addotto) Consente agli utenti di aggiornare il metodo di trattamento per attivare il raggruppamento per addotto.
Browse for files	(Ricerca file) Consente agli utenti di navigare all'esterno della cartella dati locale.
Enable standard addition	(Abilita addizione standard) Consente agli utenti di aggiornare il metodo di trattamento per attivare la funzionalità di addizione standard.
Set Manual Integration Percentage Rule	(Imposta regola percentuale di integrazione manuale) Consente agli utenti di modificare il parametro Manual Integration % .

Informazioni su utenti e ruoli

In SCIEX OS, l'amministratore può aggiungere utenti e gruppi di Windows al database User Management per SCIEX OS. Per accedere al software, gli utenti devono essere definiti nel database User Management o essere membri di un gruppo definito nel database.

Gli utenti possono essere assegnati a uno o più ruoli predefiniti, descritti nella tabella seguente, o se necessario, a ruoli personalizzati. I ruoli determinano le funzioni alle quali gli utenti hanno accesso. I ruoli predefiniti non possono essere eliminati e i diritti non possono essere modificati.

Nota: Per i gruppi di lavoro amministrati dal software Central Administrator Console (CAC), le pagine User Management sono di sola lettura.

Tabella 4-4: Ruoli predefiniti

Ruolo	Attività tipiche
Administrator (Amministratore)	<ul style="list-style-type: none"> Gestisce il sistema. Configura la sicurezza.

Controllo dell'accesso

Tabella 4-4: Ruoli predefiniti (continua)

Ruolo	Attività tipiche
Method Developer (Sviluppatore di metodi)	<ul style="list-style-type: none"> • Crea i metodi. • Esegue i lotti. • Analizza i dati che devono essere utilizzati dall'utente finale.
Analyst (Analista)	<ul style="list-style-type: none"> • Esegue i lotti. • Analizza i dati che devono essere utilizzati dall'utente finale.
Reviewer (Revisore)	<ul style="list-style-type: none"> • Controlla i dati. • Controlla gli audit trail. • Controlla i risultati della quantificazione.

Tabella 4-5: Programmare i permessi

Autorizzazione	Amministratore	Sviluppatore di metodi	Analista	Revisore
Batch (Lotto)				
Submit unlocked methods (Invia metodi sbloccati)	✓	✓	✓	×
Open (Apri)	✓	✓	✓	✓
Save as (Salva con nome)	✓	✓	✓	×
Submit (Invia)	✓	✓	✓	×
Save (Salva)	✓	✓	✓	×
Save ion reference table (Salva tabella di riferimento ionica)	✓	✓	✓	×
Add data sub-folders (Aggiungi sottocartelle dati)	✓	✓	✓	×
Configure Decision Rules (Configura regole di decisione)	✓	✓	✓	×
Configuration (Configurazione)				
General tab (Scheda Generale)	✓	✓	×	×

Tabella 4-5: Programmare i permessi (continua)

Autorizzazione	Amministratore	Sviluppatore di metodi	Analista	Revisore
General: change regional setting (Generale: modifica impostazioni generali)	✓	✓	x	x
General: full screen mode (Generale: modalità schermo intero)	✓	✓	x	x
General: Stop Windows services (Generale: arresta i servizi di Windows)	✓	x	x	x
LIMS communication tab (Scheda di comunicazione LIMS)	✓	✓	x	x
Audit maps tab (Scheda Mappe di audit)	✓	x	x	x
Queue tab (Scheda Coda)	✓	✓	✓	✓
Queue: instrument idle time (Coda: tempi di inattività strumento)	✓	✓	x	x
Queue: max number of acquired samples (Coda: numero massimo di campioni acquisiti)	✓	✓	x	x
Queue: other queue settings (Coda: altre impostazioni coda)	✓	✓	x	x
Projects tab (Scheda Progetti)	✓	✓	✓	✓
Projects: create project (Progetti: crea progetto)	✓	✓	✓	x

Tabella 4-5: Programmare i permessi (continua)

Autorizzazione	Amministratore	Sviluppatore di metodi	Analista	Revisore
Projects: apply an audit map template to an existing project (Progetti: applica un modello di mappa di audit a un progetto esistente)	✓	x	x	x
Projects: create root directory (Progetti: crea directory radice)	✓	x	x	x
Projects: set current root directory (Progetti: imposta directory radice corrente)	✓	x	x	x
Projects: specify network credentials (Progetti: specifica credenziali di rete)	✓	x	x	x
Projects: Enable checksum writing for wiff1 data creation (Progetti: abilita scrittura del checksum per la creazione di dati wiff1)	✓	x	x	x
Projects: clear root directory (Progetti: cancella directory radice)	✓	x	x	x
Devices tab (Scheda Dispositivi)	✓	✓	✓	x
User management tab (Scheda Gestione utenti)	✓	x	x	x
Force user logoff (Imponi disconnessione utente)	✓	x	x	x
Event Log (Registro eventi)				

Tabella 4-5: Programmare i permessi (continua)

Autorizzazione	Amministratore	Sviluppatore di metodi	Analista	Revisore
Access event log workspace (Accedi all'area di lavoro registro eventi)	✓	✓	✓	✓
Archive log (Archivia registro)	✓	✓	✓	✓
Audit Trail (Audit trail)				
Access audit trail workspace (Accedi all'area di lavoro audit trail)	✓	✓	✓	✓
View active audit map (Visualizza mappa di audit attiva)	✓	✓	✓	✓
Print/Export audit trail (Stampa/Esporta audit trail)	✓	✓	✓	✓
Data Acquisition Panel (Pannello di acquisizione dati)				
Start (Avvia)	✓	✓	✓	×
Stop (Arresta)	✓	✓	✓	×
Save (Salva)	✓	✓	✓	×
MS & LC Method (Metodo MS e LC)				
Access method workspace (Accedi all'area di lavoro metodo)	✓	✓	✓	✓
New (Nuovo)	✓	✓	×	×
Open (Apri)	✓	✓	✓	✓
Save (Salva)	✓	✓	×	×
Save as (Salva con nome)	✓	✓	×	×
Lock/Unlock method (Blocca/Sblocca metodo)	✓	✓	×	×
Queue (Coda)				

Controllo dell'accesso

Tabella 4-5: Programmare i permessi (continua)

Autorizzazione	Amministratore	Sviluppatore di metodi	Analista	Revisore
Manage (Gestisci)	✓	✓	✓	×
Start/Stop (Avvia/Arresta)	✓	✓	✓	×
Print (Stampa)	✓	✓	✓	✓
Library (Libreria)				
Access library workspace (Accedi all'area di lavoro libreria)	✓	✓	✓	✓
CAC settings (Client CAC)				
Enable Central Administration (Abilita amministrazione centrale)	✓	×	×	×
MS Tune (Tuning MS)				
Access MS Tune workspace (Accedi all'area di lavoro MS Tune)	✓	✓	✓	×
Advanced MS Tuning (Tuning MS avanzato)	✓	✓	×	×
Advanced troubleshooting (Risoluzione dei problemi avanzata)	✓	✓	×	×
Quick status check (Controllo rapido stato)	✓	✓	✓	×
Restore instrument data (Ripristina dati strumento)	✓	✓	×	×
Explorer (Esplora)				
Access explorer workspace (Accedi all'area di lavoro Esplora)	✓	✓	✓	✓
Export (Esporta)	✓	✓	✓	×

Tabella 4-5: Programmare i permessi (continua)

Autorizzazione	Amministratore	Sviluppatore di metodi	Analista	Revisore
Print (Stampa)	✓	✓	✓	×
Options (Opzioni)	✓	✓	✓	×
Recalibrate (Ricalibra)	✓	✓	×	×
Analytics (Analisi)				
New results (Nuovi risultati)	✓	✓	✓	×
Create processing method (Crea metodo di trattamento)	✓	✓	✓	×
Modify processing method (Modifica metodo di trattamento)	✓	✓	×	×
Allow Export and Create Report of unlocked Results Table (Consenti esportazione e creazione report della tabella risultati sbloccata)	✓	×	×	×
Save results for Automation Batch (Salva risultati per lotto automazione)	✓	✓	✓	×
Change default quantitation method integration algorithm (Modifica algoritmo di integrazione metodo di quantificazione predefinito)	✓	✓	×	×
Change default quantitation method integration parameters (Modifica parametri di integrazione metodo di quantificazione predefinito)	✓	✓	×	×

Tabella 4-5: Programmare i permessi (continua)

Autorizzazione	Amministratore	Sviluppatore di metodi	Analista	Revisore
Enable project modified peak warning (Attiva avviso picco modificato progetto)	✓	×	×	×
Add samples (Aggiungi campioni)	✓	✓	✓	×
Remove selected samples (Rimuovi campioni selezionati)	✓	✓	✓	×
Export, import, or remove external calibration (Esporta, importa o rimuovi calibrazione esterna)	✓	✓	✓	×
Modify sample name (Modifica nome campione)	✓	✓	✓	×
Modify sample type (Modifica tipo campione)	✓	✓	✓	×
Modify sample ID (Modifica ID campione)	✓	✓	✓	×
Modify actual concentration (Modifica concentrazione effettiva)	✓	✓	✓	×
Modify dilution factor (Modifica fattore di diluizione)	✓	✓	✓	×
Modify comment fields (Modifica il campo commenti)	✓	✓	✓	×
Enable manual integration (Attiva integrazione manuale)	✓	✓	✓	×

Tabella 4-5: Programmare i permessi (continua)

Autorizzazione	Amministratore	Sviluppatore di metodi	Analista	Revisore
Set peak to not found (Imposta picco su non trovato)	✓	✓	✓	×
Include or exclude a peak from the results table (Includi o escludi un picco dalla results table)	✓	✓	✓	×
Regression options (Opzioni di regressione)	✓	✓	✓	×
Modify results table integration parameters for a single chromatogram (Modifica parametri di integrazione results table per un singolo cromatogramma)	✓	✓	✓	×
Modify quantitation method for the results table component (Modifica metodo di quantificazione per il componente results table)	✓	✓	✓	×
Create metric plot new settings (Crea impostazioni nuove tracciato metrico)	✓	✓	✓	✓
Add custom columns (Aggiungi colonne personalizzate)	✓	✓	✓	×
Set peak review title format (Importa formato titolo revisione picco)	✓	×	×	×

Tabella 4-5: Programmare i permessi (continua)

Autorizzazione	Amministratore	Sviluppatore di metodi	Analista	Revisore
Remove custom column (Rimuovi colonna personalizzata)	✓	✓	×	×
Results table display settings (Impostazioni di visualizzazione Results table)	✓	✓	✓	✓
Lock results table (Blocca results table)	✓	✓	✓	✓
Unlock results table (Sblocca results table)	✓	×	×	×
Mark results file as reviewed and save (Contrassegna file di risultati come rivisti e salvati)	✓	×	×	✓
Modify report template (Modifica modello report)	✓	✓	×	×
Transfer results to LIMS (Trasferisci risultati a LIMS)	✓	✓	✓	×
Modify barcode column (Modifica colonna codice a barre)	✓	✓	×	×
Change comparison sample assignment (Modifica assegnazione campione di confronto)	✓	✓	×	×
Add the MSMS spectra to library (Aggiungi gli spettri MSMS alla libreria)	✓	✓	×	×
Project default settings (Impostazioni predefinite progetto)	✓	✓	×	×

Tabella 4-5: Programmare i permessi (continua)


Autorizzazione	Amministratore	Sviluppatore di metodi	Analista	Revisore
Create report in all formats (Crea report in tutti i formati)	✓	✓	✓	✓
Edit flagging criteria parameters (Modifica parametri dei criteri di segnalazione)	✓	✓	✓	×
Automatic outlier removal parameter change (Modifica parametro di rimozione esterna automatica)	✓	✓	×	×
Enable automatic outlier removal (Abilita rimozione esterna automatica)	✓	✓	✓	×
Update processing method via FF/LS (Aggiorna metodo di trattamento tramite FF/LS)	✓	✓	×	×
Update results via FF/LS (Aggiorna risultati tramite FF/LS)	✓	✓	×	×
Enable grouping by adducts functionality (Abilita raggruppamento per addotto)	✓	✓	×	×
Browse for files (Cerca file)	✓	✓	✓	✓
Enable standard addition (Abilita addizione standard)	✓	✓	✓	×

Tabella 4-5: Programmare i permessi (continua)

Autorizzazione	Amministratore	Sviluppatore di metodi	Analista	Revisore
Set Manual Integration Percentage Rule (Imposta regola percentuale di integrazione manuale)	✓	x	x	x

Gestione utenti

Aggiunta di un utente o un gruppo

1. Aprire l'area di lavoro Configuration.
2. Aprire la pagina User Management.
3. Aprire la scheda Users.
4. Fare clic su **Add User** ().
5. Digitare il nome di un utente o di un gruppo, quindi fare clic su **OK**.

Suggerimento! Per informazioni sulla finestra di dialogo Select User or Group e su come utilizzarla, premere **F1**.

6. Per rendere attivo un utente, accertarsi che la casella di controllo **Active user or group** sia selezionata.
7. Nell'area di lavoro **Roles**, selezionare un o più ruoli, quindi fare clic su **Save**.

Disattivazione di utenti o gruppi

1. Aprire l'area di lavoro Configuration.
2. Aprire la pagina User Management.
3. Aprire la scheda Users.
4. Nell'elenco **User name or group**, selezionare l'utente o il gruppo da disattivare.
5. Deselezionare la casella di controllo **Active user or group**.
Il software chiede conferma.
6. Fare clic su **Yes**.

Rimozione di utenti o gruppi

Seguire questa procedura per rimuovere un utente o un gruppo dal software. Se un utente o un gruppo viene rimosso da Windows, deve anche essere rimosso dal software SCIEX OS.

1. Aprire l'area di lavoro Configuration.
2. Aprire la pagina User Management.
3. Aprire la scheda Users.
4. Nell'elenco **User name or group** selezionare l'utente o il gruppo da rimuovere.
5. Fare clic su **Delete**.
Il software chiede conferma.
6. Fare clic su **OK**.


Gestione dei ruoli

Modifica dei ruoli assegnati a un utente o a un gruppo

Utilizzare questa procedura per l'assegnazione di nuovi ruoli per un utente o un gruppo, o per rimuovere le assegnazioni dei ruoli esistenti.

1. Aprire l'area di lavoro Configuration.
2. Aprire la pagina User Management.
3. Aprire la scheda Users.
4. Nel campo **User name or group** selezionare l'utente o il gruppo da modificare.
5. Selezionare i ruoli che si desidera assegnare all'utente o al gruppo ed eliminare eventuali ruoli da rimuovere.
6. Fare clic su **Save**.

Creazione di un ruolo personalizzato

1. Aprire l'area di lavoro Configuration.
2. Aprire la pagina User Management.
3. Aprire la scheda Roles.
4. Fare clic su **Add Role** ().
Verrà aperta la finestra di dialogo Duplicate a User Role.
5. Nel campo **Existing user role**, selezionare il ruolo da utilizzare come modello per il nuovo ruolo.
6. Digitare un nome e una descrizione per il ruolo e fare clic su **OK**.
7. Selezionare le autorizzazioni di accesso per il ruolo.
8. Fare clic su **Save All Roles**.
9. Fare clic su **OK**.

Eliminazione di un ruolo personalizzato

Nota: Se un utente viene assegnato solo al ruolo che verrà eliminato, il sistema richiede l'eliminazione dell'utente e del ruolo.

1. Aprire l'area di lavoro Configuration.
2. Aprire la pagina User Management.
3. Aprire la scheda Roles.
4. Fare clic su **Delete a Role**.
Viene visualizzata la finestra di dialogo Delete a User Role.
5. Selezionare il ruolo da eliminare e fare clic su **OK**.

Esportazione e importazione di impostazioni di gestione utenti

Il database di gestione utenti di SCIEX OS può essere esportato e importato. Dopo aver configurato il database User Management su un computer SCIEX, esportarlo e importarlo su altri computer SCIEX, per assicurarsi che le impostazioni di gestione utenti siano coerenti.

Vengono esportati solo gli utenti di dominio. Gli utenti locali non vengono esportati.

Prima di importare le impostazioni di gestione utenti, il software esegue automaticamente il backup delle impostazioni correnti. L'utente può ripristinare l'ultimo backup.

Esportazione di impostazioni di gestione utenti

1. Aprire l'area di lavoro Configuration.
2. Aprire la pagina User Management.
3. Fare clic su **Advanced > Export User Management settings**.
Viene visualizzata la finestra di dialogo Export User Management Settings.
4. Fare clic su **Browse**.
5. Cercare e selezionare la cartella in cui verranno salvate le impostazioni, quindi fare clic su **Select Folder**.
6. Fare clic su **Export**.
Viene mostrato un messaggio di conferma, con il nome del file che contiene le impostazioni esportate.
7. Fare clic su **OK**.

Ripristino delle impostazioni di gestione utenti

Prima di importare le impostazioni di gestione utenti, il software esegue il backup delle impostazioni correnti. Utilizzare questa procedura per ripristinare l'ultimo backup delle impostazioni di gestione utenti.

1. Aprire l'area di lavoro Configuration.

2. Aprire la pagina User Management.
3. Fare clic su **Advanced > Restore previous settings**.
Viene visualizzata la finestra di dialogo Restore User Management Settings.
4. Fare clic su **Yes**.
5. Chiudere e riaprire SCIEX OS.

Configurazione dell'accesso ai progetti e ai file di progetto

Utilizzare le funzioni di sicurezza di Windows per controllare l'accesso alla cartella SCIEX OS Data. Per impostazione predefinita, i file di progetto vengono salvati nella cartella SCIEX OS Data. Per accedere a un progetto, è necessario che gli utenti abbiano accesso alla directory radice in cui i dati del progetto sono salvati. Per ulteriori informazioni, fare riferimento alla sezione: [Configurazione di sicurezza di Windows](#).

Cartelle del progetto

Ogni progetto contiene cartelle in cui sono contenuti tipi di file diversi. Per informazioni sul contenuto di cartelle diverse, fare riferimento alla tabella: [Tabella 4-6](#).

Tabella 4-6: Cartelle del progetto

Cartella	Contenuto
\Acquisition Methods	Contiene i metodi LC e MS (spettrometro di massa) creati nel progetto. I metodi MS presentano l'estensione msm, mentre i metodi LC presentano l'estensione lcm.
\Audit Data	Contiene la mappa di audit del progetto e tutte le informazioni di ispezione.
\Batch	Contiene tutti i file di acquisizione lotto che sono stati salvati. I lotti di acquisizione hanno l'estensione bch.
\Data	Contiene i file dei dati di acquisizione. I file di dati di acquisizione hanno le estensioni wiff e wiff2.
\Project Information	Contiene i file delle impostazioni predefinite del progetto.
\Quantitation Methods	Contiene tutti i file dei metodi di elaborazione. I metodi di elaborazione hanno l'estensione qmethod
\Quantitation Results	Contiene tutti i file della Results Table di quantificazione. I file della Results Table presentano l'estensione qsession.

Tipi di file del software

Per i tipi di file comuni di SCIEX OS, fare riferimento alla tabella: [Tabella 4-7](#).

Tabella 4-7: File di SCIEX OS

Estensione	Tipo di file	Cartella
atds	<ul style="list-style-type: none"> Dati audit trail workstation e archivi Impostazioni degli audit trail della workstation Dati relativi agli audit trail del progetto e archivi Impostazioni per gli audit trail del progetto 	<ul style="list-style-type: none"> Per i progetti: <project name>\Audit Data Per la workstation: C:\ProgramData\SCIEX\Audit Data
atms	Mappe di audit	<ul style="list-style-type: none"> Per i progetti: <project name>\Audit Data Per la workstation: C:\ProgramData\SCIEX\Audit Data
bch	Lotto	Batch
cset	Impostazioni Results Table	Project Information
dad	File di dati relativi alla spettrometria di massa	<ul style="list-style-type: none"> Optimization Data
exml	Project default settings	Project Information
Journal of	File temporanei creati da SCIEX OS	Varie cartelle
lcm	Metodo LC	Acquisition Methods
msm	Metodo MS	Acquisition Methods
pdf	Dati Portable Document Format	—
qlayout	Layout dell'area di lavoro	— Nota: Il layout dell'area di lavoro predefinito per un progetto viene archiviato nella cartella Project Information.
qmethod	Metodo di elaborazione	Quantitation Methods

Tabella 4-7: File di SCIEX OS (continua)

Estensione	Tipo di file	Cartella
qsession	Results Table del software Results Table Nota: SCIEX OS può solo aprire file qsession creati con SCIEX OS.	Quantitation Results
wiff	File di dati di spettrometria di massa compatibili con il software SCIEX OS Nota: SCIEX OS genera file wiff e wiff2.	Data
wiff.scan	File di dati relativi alla spettrometria di massa	<ul style="list-style-type: none"> • Optimization • Data
wiff2	File di dati relativi alla spettrometria di massa generati da SCIEX OS	<ul style="list-style-type: none"> • Optimization • Data
xls oxlsx	Foglio Excel	Batch
xps	Ricalibrazione	Data\Cal

Il software Central Administrator Console (CAC) è un'alternativa opzionale all'amministrazione locale con il software SCIEX OS. Il software CAC contiene la personalizzazione e la gestione per ruolo centrale, utente, workstation e gruppo di lavoro, tutto in una sola applicazione.

Questa sezione descrive il software CAC e spiega come configurarlo e utilizzarlo per gestire centralmente persone, progetti e workstation.

Nota: Per utilizzare il software CAC e registrare le workstation con il server, assicurarsi che il software SCIEX OS sia installato su ogni workstation.

Il software CAC è abilitato tramite licenza e può essere installato in qualsiasi workstation in grado di supportare SCIEX OS versione 3.0 e Windows Server 2019.

Il software CAC è incluso nel pacchetto di installazione di SCIEX OS. Tuttavia, non è possibile installare il software CAC e SCIEX OS sulla stessa workstation.


Utenti

Utilizzare la pagina User Management per aggiungere utenti e gruppi di Windows al database User Management per SCIEX OS. L'amministratore può anche aggiungere, modificare ed eliminare ruoli utente nella sezione User Roles and Permissions. Per accedere al software, gli utenti devono essere definiti nel database User Management o essere membri di un gruppo definito nel database.

Pool utenti

Solo gli utenti autorizzati possono connettersi alla workstation e accedere a SCIEX OS quando SCIEX OS viene gestito con il software Central Administrator Console (CAC). Prima di poter essere aggiunti ai gruppi di lavoro, gli utenti devono essere aggiunti al pool utenti.

Aggiunta di un utente o gruppo al pool utenti

1. Aprire l'area di lavoro Central Administration.
2. Aprire la pagina User Management.
3. Aprire la scheda User Pool.
4. Fare clic su **Add users to the User Pool** ().
Viene visualizzata la finestra di dialogo Select Users or Groups.
5. Digitare il nome di un utente o di un gruppo, quindi fare clic su **OK**.

Suggerimento! Tenere premuto il tasto **Ctrl** e fare clic su **OK** per selezionare più utenti o gruppi.

Eliminazione di utenti o gruppi

1. Aprire l'area di lavoro Central Administration.
2. Aprire la pagina User Management.
3. Aprire la scheda User Pool.
4. Nel riquadro destro, selezionare l'utente o il gruppo da eliminare, quindi fare clic su **Delete**.
Il software chiede conferma.
5. Fare clic su **OK**.

Ruoli utente e autorizzazioni

Questa sezione descrive la pagina User Roles and Permissions.

Gli utenti possono essere assegnati a uno o più ruoli predefiniti, descritti nella tabella seguente, o se necessario, a ruoli personalizzati. I ruoli determinano le funzioni alle quali gli utenti hanno accesso. I ruoli predefiniti non possono essere eliminati e le relative autorizzazioni non possono essere modificate.

Tabella 5-1: Ruoli predefiniti

Ruolo	Attività tipiche
Administrator (Amministratore)	<ul style="list-style-type: none"> • Gestisce il sistema. • Configura la sicurezza.
Method Developer (Sviluppatore di metodi)	<ul style="list-style-type: none"> • Crea i metodi. • Esegue i lotti. • Analizza i dati che devono essere utilizzati dall'utente finale.
Analyst (Analista)	<ul style="list-style-type: none"> • Esegue i lotti. • Analizza i dati che devono essere utilizzati dall'utente finale.
Reviewer (Revisore)	<ul style="list-style-type: none"> • Controlla i dati. • Controlla gli audit trail. • Controlla i risultati della quantificazione.

Tabella 5-2: Programmare i permessi

Autorizzazione	Amministratore	Sviluppatore di metodi	Analista	Revisore
Batch (Lotto)				

Central Administrator Console

Tabella 5-2: Programmare i permessi (continua)

Autorizzazione	Amministratore	Sviluppatore di metodi	Analista	Revisore
Submit unlocked methods (Invia metodi sbloccati)	✓	✓	✓	×
Open (Apri)	✓	✓	✓	✓
Save as (Salva con nome)	✓	✓	✓	×
Submit (Invia)	✓	✓	✓	×
Save (Salva)	✓	✓	✓	×
Save ion reference table (Salva tabella di riferimento ionica)	✓	✓	✓	×
Add data sub-folders (Aggiungi sottocartelle dati)	✓	✓	✓	×
Configure Decision Rules (Configura regole di decisione)	✓	✓	✓	×
Configuration (Configurazione)				
General tab (Scheda Generale)	✓	✓	×	×
General: change regional setting (Generale: modifica impostazioni generali)	✓	✓	×	×
General: full screen mode (Generale: modalità schermo intero)	✓	✓	×	×
LIMS communication tab (Scheda di comunicazione LIMS)	✓	✓	×	×
General: Stop Windows services (Generale: arretra i servizi di Windows)	✓	×	×	×

Tabella 5-2: Programmare i permessi (continua)

Autorizzazione	Amministratore	Sviluppatore di metodi	Analista	Revisore
Audit maps tab (Scheda Mappe di audit)	✓	×	×	×
Queue tab (Scheda Coda)	✓	✓	✓	✓
Queue: instrument idle time (Coda: tempi di inattività strumento)	✓	✓	×	×
Queue: max number of acquired samples (Coda: numero massimo di campioni acquisiti)	✓	✓	×	×
Queue: other queue settings (Coda: altre impostazioni coda)	✓	✓	×	×
Projects tab (Scheda Progetti)	✓	✓	✓	✓
Projects: create project (Progetti: crea progetto)	✓	✓	✓	×
Projects: apply an audit map template to an existing project (Progetti: applica un modello di mappa di audit a un progetto esistente)	✓	×	×	×
Projects: create root directory (Progetti: crea directory radice)	✓	×	×	×
Projects: set current root directory (Progetti: imposta directory radice corrente)	✓	×	×	×

Tabella 5-2: Programmare i permessi (continua)

Autorizzazione	Amministratore	Sviluppatore di metodi	Analista	Revisore
Projects: specify network credentials (Progetti: specifica credenziali di rete)	✓	×	×	×
Projects: Enable checksum writing for wiff1 data creation (Progetti: abilita scrittura del checksum per la creazione di dati wiff1)	✓	×	×	×
Projects: clear root directory (Progetti: cancella directory radice)	✓	×	×	×
Devices tab (Scheda Dispositivi)	✓	✓	✓	×
User management tab (Scheda Gestione utenti)	✓	×	×	×
Force user logoff (Imponi disconnessione utente)	✓	×	×	×
Event Log (Registro eventi)				
Access event log workspace (Accedi all'area di lavoro registro eventi)	✓	✓	✓	✓
Archive log (Archivia registro)	✓	✓	✓	✓
Audit Trail (Audit trail)				
Access audit trail workspace (Accedi all'area di lavoro audit trail)	✓	✓	✓	✓
View active audit map (Visualizza mappa di audit attiva)	✓	✓	✓	✓

Tabella 5-2: Programmare i permessi (continua)

Autorizzazione	Amministratore	Sviluppatore di metodi	Analista	Revisore
Print/Export audit trail (Stampa/Esporta audit trail)	✓	✓	✓	✓
Data Acquisition Panel (Pannello di acquisizione dati)				
Start (Avvia)	✓	✓	✓	×
Stop (Arresta)	✓	✓	✓	×
Save (Salva)	✓	✓	✓	×
MS & LC Method (Metodo MS e LC)				
Access method workspace (Accedi all'area di lavoro metodo)	✓	✓	✓	✓
New (Nuovo)	✓	✓	×	×
Open (Apri)	✓	✓	✓	✓
Save (Salva)	✓	✓	×	×
Save as (Salva con nome)	✓	✓	×	×
Lock/Unlock method (Blocca/Sblocca metodo)	✓	✓	×	×
Queue (Coda)				
Manage (Gestisci)	✓	✓	✓	×
Start/Stop (Avvia/Arresta)	✓	✓	✓	×
Print (Stampa)	✓	✓	✓	✓
Library (Libreria)				
Access library workspace (Accedi all'area di lavoro libreria)	✓	✓	✓	✓
CAC settings (Client CAC)				

Central Administrator Console

Tabella 5-2: Programmare i permessi (continua)

Autorizzazione	Amministratore	Sviluppatore di metodi	Analista	Revisore
Enable Central Administration (Abilita amministrazione centrale)	✓	×	×	×
MS Tune (Tuning MS)				
Access MS Tune workspace (Accedi all'area di lavoro MS Tune)	✓	✓	✓	×
Advanced MS Tuning (Tuning MS avanzato)	✓	✓	×	×
Advanced troubleshooting (Risoluzione dei problemi avanzata)	✓	✓	×	×
Quick status check (Controllo rapido stato)	✓	✓	✓	×
Restore instrument data (Ripristina dati strumento)	✓	✓	×	×
Analytics (Analisi)				
New results (Nuovi risultati)	✓	✓	✓	×
Create processing method (Crea metodo di trattamento)	✓	✓	✓	×
Modify processing method (Modifica metodo di trattamento)	✓	✓	×	×
Allow Export and Create Report of unlocked Results Table (Consenti esportazione e creazione report della tabella risultati sbloccata)	✓	×	×	×

Tabella 5-2: Programmare i permessi (continua)

Autorizzazione	Amministratore	Sviluppatore di metodi	Analista	Revisore
Save results for Automation Batch (Salva risultati per lotto automazione)	✓	✓	✓	×
Change default quantitation method integration algorithm (Modifica algoritmo di integrazione metodo di quantificazione predefinito)	✓	✓	×	×
Change default quantitation method integration parameters (Modifica parametri di integrazione metodo di quantificazione predefinito)	✓	✓	×	×
Enable project modified peak warning (Attiva avviso picco modificato progetto)	✓	×	×	×
Add samples (Aggiungi campioni)	✓	✓	✓	×
Remove selected samples (Rimuovi campioni selezionati)	✓	✓	✓	×
Export, import, or remove external calibration (Esporta, importa o rimuovi calibrazione esterna)	✓	✓	✓	×
Modify sample name (Modifica nome campione)	✓	✓	✓	×
Modify sample type (Modifica tipo campione)	✓	✓	✓	×

Tabella 5-2: Programmare i permessi (continua)

Autorizzazione	Amministratore	Sviluppatore di metodi	Analista	Revisore
Modify sample ID (Modifica ID campione)	✓	✓	✓	×
Modify actual concentration (Modifica concentrazione effettiva)	✓	✓	✓	×
Modify dilution factor (Modifica fattore di diluizione)	✓	✓	✓	×
Modify comment fields (Modifica il campo commenti)	✓	✓	✓	×
Enable manual integration (Attiva integrazione manuale)	✓	✓	✓	×
Set peak to not found (Imposta picco su non trovato)	✓	✓	✓	×
Include or exclude a peak from the results table (Includi o escludi un picco dalla results table)	✓	✓	✓	×
Regression options (Opzioni di regressione)	✓	✓	✓	×
Modify results table integration parameters for a single chromatogram (Modifica parametri di integrazione results table per un singolo cromatogramma)	✓	✓	✓	×

Tabella 5-2: Programmare i permessi (continua)

Autorizzazione	Amministratore	Sviluppatore di metodi	Analista	Revisore
Modify quantitation method for the results table component (Modifica metodo di quantificazione per il componente results table)	✓	✓	✓	×
Create metric plot new settings (Crea impostazioni nuove tracciato metrico)	✓	✓	✓	✓
Add custom columns (Aggiungi colonne personalizzate)	✓	✓	✓	×
Set peak review title format (Importa formato titolo revisione picco)	✓	×	×	×
Remove custom column (Rimuovi colonna personalizzata)	✓	✓	×	×
Results table display settings (Impostazioni di visualizzazione Results table)	✓	✓	✓	✓
Lock results table (Blocca results table)	✓	✓	✓	✓
Unlock results table (Sblocca results table)	✓	×	×	×
Mark results file as reviewed and save (Contrassegna file di risultati come rivisti e salvati)	✓	×	×	✓
Modify report template (Modifica modello report)	✓	✓	×	×

Tabella 5-2: Programmare i permessi (continua)

Autorizzazione	Amministratore	Sviluppatore di metodi	Analista	Revisore
Transfer results to LIMS (Trasferisci risultati a LIMS)	✓	✓	✓	×
Modify barcode column (Modifica colonna codice a barre)	✓	✓	×	×
Change comparison sample assignment (Modifica assegnazione campione di confronto)	✓	✓	×	×
Add the MSMS spectra to library (Aggiungi gli spettri MSMS alla libreria)	✓	✓	×	×
Project default settings (Impostazioni predefinite progetto)	✓	✓	×	×
Create report in all formats (Crea report in tutti i formati)	✓	✓	✓	✓
Edit flagging criteria parameters (Modifica parametri dei criteri di segnalazione)	✓	✓	✓	×
Automatic outlier removal parameter change (Modifica parametro di rimozione esterna automatica)	✓	✓	×	×
Enable automatic outlier removal (Abilita rimozione esterna automatica)	✓	✓	✓	×
Update processing method via FF/LS (Aggiorna metodo di trattamento tramite FF/LS)	✓	✓	×	×


Tabella 5-2: Programmare i permessi (continua)

Autorizzazione	Amministratore	Sviluppatore di metodi	Analista	Revisore
Update results via FF/LS (Aggiorna risultati tramite FF/LS)	✓	✓	×	×
Enable grouping by adducts functionality (Abilita raggruppamento per addotto)	✓	✓	×	×
Browse for files (Cerca file)	✓	✓	✓	✓
Enable standard addition (Abilita addizione standard)	✓	✓	✓	×
Set Manual Integration Percentage Rule (Imposta regola percentuale di integrazione manuale)	✓	×	×	×
Explorer (Esplora)				
Access explorer workspace (Accedi all'area di lavoro Esplora)	✓	✓	✓	✓
Export (Esporta)	✓	✓	✓	×
Print (Stampa)	✓	✓	✓	×
Options (Opzioni)	✓	✓	✓	×
Recalibrate (Ricalibra)	✓	✓	×	×

Aggiunta di un ruolo personalizzato

Il software Central Administrator Console (CAC) prevede quattro ruoli predefiniti. Se sono necessari ulteriori ruoli, copiare un ruolo esistente e assegnare a esso diritti di accesso.

1. Aprire l'area di lavoro Central Administration.
2. Aprire la pagina User Management.
3. Aprire la scheda User Roles and Permissions.

4. Fare clic su **Add Role** ().
Verrà aperta la finestra di dialogo Duplicate a User Role.
5. Nel campo **Existing user role**, selezionare il ruolo da utilizzare come modello per il nuovo ruolo.
6. Digitare un nome e una descrizione per il ruolo e fare clic su **OK**.
Il nuovo ruolo viene mostrato nella finestra User Roles and Permission Categories.
7. Selezionare i privilegi di accesso per il ruolo selezionando le caselle di controllo appropriate.
8. Fare clic su **Save All Roles**.

Eliminazione di un ruolo personalizzato

1. Aprire l'area di lavoro Central Administration.
2. Aprire la pagina User Management.
3. Aprire la scheda User Roles and Permissions.
4. Fare clic su **Delete a Role**.
Viene visualizzata la finestra di dialogo Delete a User Role.
5. Selezionare il ruolo da eliminare e fare clic su **OK**.

Gruppi di lavoro

Utilizzare la pagina Workgroup Management per gestire i gruppi di lavoro. I gruppi di lavoro contengono utenti, workstation e progetti.

Creare un gruppo di lavoro aggiungendo risorse dai rispettivi pool. Prima di creare gruppi di lavoro, assicurarsi di aggiungere tutti gli utenti potenziali al pool utenti, le workstation al pool workstation e le directory radice dei progetti al pool progetti.

Se necessario, aggiungere altri ruoli. Se lo si desidera, selezionare la modalità di sicurezza per ogni gruppo di lavoro.


L'impostazione della modalità di sicurezza per il gruppo di lavoro prevale sull'impostazione della modalità di sicurezza della workstation se la workstation è registrata nel software Central Administrator Console (CAC) ed è un membro del gruppo di lavoro.

Non aggiungere utenti locali ai gruppi di lavoro. Il software CAC è un'applicazione di rete e solo gli utenti di rete devono essere aggiunti al gruppo di lavoro.

Nota: In ogni gruppo di lavoro, è necessario assegnare ad almeno un utente il ruolo di amministratore. Solo un amministratore o supervisore può sbloccare lo schermo del software CAC se l'utente attualmente connesso non è disponibile.

Se la sicurezza basata sul server non è più necessaria per una particolare workstation, gestire localmente la sicurezza per la workstation con SCIEX OS.

Creazione di un gruppo di lavoro

1. Aprire l'area di lavoro Central Administration.
2. Aprire la pagina Workgroup Management.
3. Fare clic su **Add Workgroup** ().
Viene visualizzata la finestra di dialogo Add a Workgroup .
4. Inserire un nome nel campo **Workgroup Name**.
5. Digitare una descrizione nel campo **Description**, quindi fare clic su **Add**.
Il gruppo di lavoro viene creato e aggiunto al riquadro Manage Workgroups and Assignments. Il software Central Administrator Console (CAC) crea il nome del gruppo di lavoro appropriato sul server.

Nota: La modalità Integrated è l'impostazione di sicurezza predefinita.


Eliminazione di un gruppo di lavoro

Se un gruppo di lavoro non è più necessario, eliminarlo dall'elenco dei gruppi di lavoro. Quando si elimina un gruppo di lavoro, lo si elimina solo dal software Central Administrator Console (CAC). Nessun dato della workstation andrà perduto.

1. Aprire l'area di lavoro Central Administration.
2. Aprire la pagina Workgroup Management.
3. Espandere l'elenco **Workgroups** e trovare il gruppo di lavoro da eliminare. Fare clic su **Delete**.
Verrà visualizzata la finestra di dialogo Delete Workgroup.
4. Fare clic su **Yes**.

Aggiunta di utenti o gruppi a un gruppo di lavoro

Nota: Agli utenti aggiunti al gruppo di lavoro non viene assegnato un ruolo automaticamente. Per assegnare ruoli agli utenti, fare riferimento alla sezione: [Aggiunta o rimozione di un ruolo](#).

1. Aprire l'area di lavoro Central Administration.
2. Aprire la pagina Workgroup Management.
3. Nel riquadro Manage Workgroups and Assignments, espandere il gruppo di lavoro da modificare, quindi espandere l'elenco **Users**.
4. Selezionare un utente o un gruppo, quindi fare clic su **Add** ().

Suggerimento! Aggiungere o selezionare più utenti premendo **Shift** e selezionando gli utenti necessari.

L'utente o il gruppo viene aggiunto al gruppo di lavoro corrente.

Central Administrator Console

5. Assegnare uno o più ruoli all'utente o al gruppo aggiunto. Fare riferimento alla sezione: [Aggiunta o rimozione di un ruolo](#).
6. Fare clic su **Save**.

Aggiunta o rimozione di un ruolo


Procedure preliminari
<ul style="list-style-type: none">• Aggiunta di utenti o gruppi a un gruppo di lavoro.

Per informazioni sulla creazione di ruoli nel software Central Administrator Console (CAC), fare riferimento alla sezione: [Aggiunta di un ruolo personalizzato](#). Gli utenti o i gruppi con un ruolo assegnato dispongono di tutte le autorizzazioni associate al ruolo. Gli utenti o i gruppi possono avere più di un ruolo alla volta.

1. Aprire l'area di lavoro Central Administration.
2. Aprire la pagina Workgroup Management.
3. Nel riquadro Manage Workgroups and Assignments, espandere il gruppo di lavoro da modificare, quindi espandere l'elenco **Users**.
4. Nella sezione Current Workgroup Membership, assegnare o rimuovere ruoli nella colonna **Assign Roles**.
5. Fare clic su **Save**.

Aggiunta di workstation a un gruppo di lavoro

Nota: Una workstation viene mostrata nel relativo pool solo se è stata registrata con il software Central Administrator Console (CAC). Fare riferimento alla sezione: [Aggiunta di una workstation](#)

1. Aprire l'area di lavoro Central Administration.
2. Aprire la pagina Workgroup Management.
3. Nel riquadro Manage Workgroups and Assignments, espandere il gruppo di lavoro da modificare, quindi espandere l'elenco **Workstations**.
4. Selezionare una workstation, quindi fare clic su **Add** ().
La workstation viene aggiunta al gruppo di lavoro corrente.
5. Fare clic su **Save**.

Assegnazione di impostazioni di sicurezza gruppo di lavoro

Procedure preliminari
<ul style="list-style-type: none">• Aggiunta di una workstation• Aggiunta di workstation a un gruppo di lavoro


Per informazioni sulle modalità di sicurezza, fare riferimento alla sezione: [Configurazione della modalità di protezione](#).

1. Aprire l'area di lavoro Central Administration.
2. Aprire la pagina Workgroup Management.
3. Nel riquadro Manage Workgroups and Assignments, espandere il gruppo di lavoro da modificare, quindi espandere l'elenco **Workstations**.
4. (Opzionale) Per impostare come predefinito il gruppo di lavoro corrente per quella workstation, selezionare la casella di controllo **Set Default** nella sezione Current Workgroup Membership.
5. Nella sezione Assign Security Settings, selezionare la **Security mode** per il gruppo di lavoro, quindi digitare l'ora appropriata per **Screen lock** e **Auto logoff**.
6. Fare clic su **Save**.

Aggiunta di progetti a un gruppo di lavoro

Nota: Questa procedura è necessaria solo se l'accesso al progetto viene gestito centralmente.

Nota: Se un progetto viene aggiunto a più gruppi di lavoro, l'accesso utenti al progetto viene allegato, non sovrascritto. Ad esempio, il gruppo di lavoro 1 comprende l'utente A, l'utente B e Project_01. Il gruppo di lavoro 2 comprende l'Utente B e l'Utente C. Se Project_01 viene aggiunto al gruppo di lavoro 2, l'Utente A, l'Utente B e l'Utente C avranno tutti accesso a Project_01.

1. Aprire l'area di lavoro Central Administration.
2. Aprire la pagina Workgroup Management.
3. Nel riquadro Manage Workgroups and Assignments, espandere il gruppo di lavoro da modificare, quindi espandere l'elenco **Projects**.
4. Selezionare la casella di controllo **Use central settings for projects**. Viene mostrata la sezione di selezione del progetto.
5. Selezionare una **Project root directory** per aggiungere un intero gruppo di progetti o espandere la cartella radice del progetto e selezionare un progetto specifico da aggiungere al gruppo di lavoro.
6. Fare clic su **Add** () per aggiungere i progetti al gruppo di lavoro. La cartella radice del progetto viene aggiunta alla tabella Current Workgroup Membership. Espandere la cartella radice del progetto per mostrare i progetti correnti nel gruppo di lavoro.
7. Fare clic su **Save**.

Gestione dei progetti

Utilizzare la pagina Project Management per creare, modificare ed eliminare progetti.

Per accedere a un progetto, è necessario che gli utenti abbiano accesso alla directory radice in cui i dati del progetto sono salvati. Per ulteriori informazioni, fare riferimento alla sezione: [Informazioni su progetti e directory radice](#).

Informazioni su progetti e directory radice

Una directory radice è una cartella che contiene uno o più progetti. È la cartella in cui il software cerca i dati dei progetti. La directory radice predefinita è `D:\SCIEX OS Data`.

Per garantire un salvataggio sicuro delle informazioni del progetto, creare i progetti utilizzando il software Central Administrator Console (CAC). Aggiungere progetti al Project Root Pool prima di aggiungerli a un gruppo di lavoro. Fare riferimento alla sezione: [Aggiunta di un progetto](#).

I dati di progetto possono essere organizzati in sottocartelle. Creare le sottocartelle con il software CAC. Fare riferimento alla sezione: [Aggiunta di una sottocartella](#).

Nota: Se un progetto viene creato all'esterno del software CAC, la directory radice del progetto deve essere aggiornata dopo la creazione del progetto. Quando si aggiorna la directory radice, il contenuto del Project Root Pool viene sincronizzato con il contenuto delle directory radice del progetto in rete.

Aggiunta di una directory radice

La directory radice è la cartella in cui vengono memorizzati uno o più progetti.

Nota: Il software può salvare fino a dieci directory radice.

Suggerimento! Le unità locali non sono accessibili in rete. Una directory radice può essere creata solo in un'unità condivisa.

1. Aprire l'area di lavoro Central Administration.
2. Aprire la pagina Project Management.
3. Fare clic su **Add new or existing project root to project pool** (). Viene visualizzata la finestra di dialogo Add Root Directory.
4. Digitare il percorso completo della directory radice, quindi fare clic su **OK**. La cartella è stata creata.

Suggerimento! Aniché digitare il percorso, fare clic su **Browse** e selezionare la cartella nella quale sarà creata la directory radice.

Suggerimento! In alternativa, creare una cartella in File Explorer, navigare fino a e selezionare la cartella.

Nota: Per le installazioni di SCIEX OS con una licenza di elaborazione, la directory radice può essere una cartella del software Analyst (`Analyst Data\Projects`).

5. Fare clic su **OK**.
La nuova directory radice diventa la directory radice del progetto attuale.

Eliminazione di una directory radice del progetto

Il software mantiene un elenco delle ultime dieci directory radice utilizzate. L'utente può eliminare le directory radice da questo elenco.

Nota: Eliminando una directory radice del progetto si eliminano anche tutti i progetti associati dal pool delle directory radici del progetto.

1. Aprire l'area di lavoro Central Administration.
2. Aprire la pagina Project Management.
3. Trovare la directory radice del progetto da eliminare, quindi fare clic su **Delete Project Root** nella sezione Actions.
Il software chiede conferma.
4. Fare clic su **OK**.

Aggiunta di un progetto

Procedure preliminari
<ul style="list-style-type: none">• Aggiunta di una directory radice

Il progetto memorizza metodi di acquisizione, dati, lotti, metodi di trattamento, risultati di elaborazione e così via. È consigliabile usare una cartella separata per ciascun progetto.


Non creare progetti o copiare o incollare file all'esterno del software Central Administrator Console (CAC).

1. Aprire l'area di lavoro Central Administration.
2. Aprire la pagina Project Management.
3. Fare clic su **Add project** nella sezione Actions della cartella radice.
Viene visualizzata la finestra di dialogo New Project.
4. Digitare il nome del progetto.
5. Fare clic su **OK**.
Il nuovo progetto viene mostrato nella cartella radice del progetto.


Aggiunta di una sottocartella

I dati nei progetti possono essere ulteriormente organizzati in sottocartelle.

1. Aprire l'area di lavoro Central Administration.
2. Aprire la pagina Project Management.
3. Fare clic su **Add data sub-folders** nella sezione Actions della cartella radice.
Viene visualizzata la finestra di dialogo Add Data Sub-Folders.

4. Selezionare un progetto a cui apparterrà la sottocartella.
5. Fare clic su **Add a new data sub-folder** ().
Viene visualizzata la finestra di dialogo Data Sub-Folder Name.
6. Digitare il nome della sottocartella
7. Fare clic su **Save**.

Suggerimento! Le sottocartelle possono essere annidate all'interno di altre sottocartelle. Per creare una sottocartella annidata, selezionare una sottocartella esistente nella sezione Project Data Sub-Folders, quindi fare clic su **Add a new data**

sub-folder ().


8. Chiudere la finestra di dialogo Add Data Sub-Folders.

Workstation

Utilizzare la pagina Workstation Management per gestire tutte le workstation connesse al server CAC. Alle workstation controllate dal software CAC vengono applicate automaticamente impostazioni personalizzate.

Aggiunta di una workstation

Nella pagina Workstation Management, gli amministratori possono aggiungere o rimuovere workstation dal controllo del software Central Administrator Console (CAC).

1. Aprire l'area di lavoro Central Administration.
2. Aprire la pagina Workstation Management.
3. Fare clic su **Add Workstation to the Workstations Pool** ().
Viene visualizzata la finestra di dialogo Select Computers.
4. Digitare i nomi delle workstation da aggiungere, quindi fare clic su **OK**.

Eliminazione di una workstation

Se una workstation non è più in uso o non è più necessario che faccia parte di un gruppo di lavoro, eliminarla dal pool delle workstation. Quando si elimina una workstation, la si rimuove da qualsiasi gruppo di lavoro a cui era assegnata. Una volta rimossa la workstation, nessuno dei dati su di essa memorizzati andrà perduto.

1. Aprire l'area di lavoro Central Administration.
2. Aprire la pagina Workstation Management.
3. Fare clic su **Workstation Management**.

4. Nel riquadro Workstation Pool trovare la workstation da eliminare, quindi fare clic su **Delete**.
Verrà visualizzata la finestra di dialogo Delete Workstation .
5. Fare clic su **OK**.

Report e funzionalità di sicurezza

Generazione di report di dati del gruppo di lavoro

Gli utenti possono generare report di dati che includono dettagli come gli utenti, i ruoli, le workstation, i progetti e i gruppi di lavoro configurati.

1. Aprire l'area di lavoro Central Administration.
2. Fare clic su **Print**.
Si apre la finestra di dialogo Print.
3. Impostare le opzioni di stampa e fare clic su **Print**.
4. (Solo Stampa su PDF) Spostarsi sul percorso in cui il report verrà salvato, quindi fare clic su **Save**.

Esportazione delle impostazioni software CAC

L'utente può esportare le impostazioni di sicurezza che è possibile applicare a un altro server Central Administrator Console (CAC). Le impostazioni sono esportate come file ecac.

1. Aprire l'area di lavoro Central Administration.
2. Fare clic su **Advanced > Export CAC settings**.
Viene visualizzata la finestra di dialogo Export CAC Settings.
3. Fare clic su **Browse**.
4. Cercare e selezionare la cartella in cui verranno salvate le impostazioni, quindi fare clic su **Select Folder**.
5. Fare clic su **Export**.
Viene mostrato un messaggio di conferma, con il nome del file che contiene le impostazioni esportate.
6. Fare clic su **OK**.

Importazione delle impostazioni software CAC

Procedure preliminari
<ul style="list-style-type: none">• Esportazione delle impostazioni software CAC

L'utente può importare le impostazioni di sicurezza da SCIEX OS o da altri server Central Administrator Console (CAC). Le impostazioni sono importate da un file ecac.

1. Aprire l'area di lavoro Central Administration.

Central Administrator Console

2. Fare clic su **Advanced > Import CAC settings**.
Viene visualizzata la finestra di dialogo Import CAC Settings.
3. Fare clic su **Browse**.
4. Cercare e selezionare il file che contiene le impostazioni da importare, quindi fare clic su **Open**.
Il software verifica che il file sia valido.
5. Fare clic su **Import**.
Il software esegue il backup delle impostazioni correnti e importa quelle nuove. Viene visualizzato un messaggio di conferma.

Nota: Le impostazioni importate vengono applicate dopo il riavvio del software CAC.

6. Fare clic su **OK**.

Ripristino delle impostazioni CAC

L'utente può importare automaticamente le impostazioni eac esportate più di recente.

1. Aprire l'area di lavoro Central Administration.
2. Fare clic su **Advanced > Restore CAC settings**.
Viene visualizzata la finestra di dialogo Restore CAC Settings.

Nota: Le impostazioni ripristinate vengono applicate con il riavvio del software Central Administrator Console (CAC).

3. Fare clic su **Yes**.

In questa sezione vengono descritti il funzionamento dell'acquisizione di rete nel software SCIEX OS e i vantaggi e le limitazioni dei progetti basati su rete. Vengono inoltre illustrate le procedure per la configurazione dell'acquisizione di rete.

Informazioni sull'acquisizione di rete

L'acquisizione di rete può essere utilizzata per acquisire dati da uno o più strumenti in cartelle di progetto di rete che è possibile elaborare da stazioni di lavoro remote. Questo processo tollera gli errori di rete e verifica che non vengano persi dei dati se si verifica un errore di connessione di rete durante l'acquisizione.

Le prestazioni del sistema possono essere inferiori quando sono utilizzati i progetti in rete rispetto a quando sono utilizzati i progetti locali. Poiché alcuni audit trail si trovano anche nelle cartelle in rete, qualsiasi attività che genera un report di controllo del progetto è rallentata. L'apertura dei file in rete potrebbe richiedere un po' di tempo, in base alle prestazioni della rete. Le prestazioni della rete sono correlate non solo all'hardware fisico della rete, ma anche al traffico in rete e alla sua configurazione.

Nota: Se il servizio ClearCore2 viene interrotto durante l'acquisizione in rete, i dati parziali del campione in acquisizione nel momento dell'interruzione non saranno scritti nel file di dati.

Nota: quando si utilizza l'acquisizione in rete in un ambiente regolamentato, sincronizzare l'orologio del computer locale con quello del server per timestamp precisi. L'orario del server viene usato per l'ora di creazione del file. Audit Trail Manager registra l'ora di creazione del file usando l'orario del computer locale.

ATTENZIONE: Rischio di perdita di dati. Non salvare i dati di più computer di acquisizione nello stesso file di dati di rete.

Vantaggi che comporta l'uso dell'acquisizione di rete

L'acquisizione dei dati di rete fornisce un metodo di lavoro sicuro con le cartelle del progetto che si trovano interamente sui server di rete. In questo modo si riduce la complessità legata alla raccolta di dati a livello locale e quindi nello spostamento dei dati in una posizione della rete per la conservazione. Inoltre, poiché il backup delle unità di rete avviene in genere automaticamente, non è quasi mai necessario eseguire il backup di unità locali.

Account di rete sicuro

In un ambiente regolamentato dove i dati vengono acquisiti in una cartella di rete, è consigliabile che gli utenti non abbiano diritti di eliminazione per la cartella di destinazione.

Acquisizione di rete

Tuttavia, senza accesso con diritti di eliminazione a questa cartella, le prestazioni di SCIEX OS non sono ottimali. La funzionalità account di rete sicuro (SNA) identifica un account di rete che dispone dell'autorizzazione file Full Control per la directory radice di rete. Il servizio ClearCore2 utilizza questo account per trasferire i dati nella cartella di rete.

L'account SNA deve avere l'autorizzazione Full Control per:

- La cartella della directory radice di rete
- La cartella SCIEX OS Data\NetworkBackup sul computer di acquisizione
- La cartella SCIEX OS Data\TempData sul computer di acquisizione

Non è necessario che l'account SNA:

- Appartenga al gruppo Administrator sul computer.
- Si trovi nel database User Management di SCIEX OS.

Lo SNA è specificato nella pagina Projects nell'area di lavoro Configuration. È possibile specificare un solo account di dominio o di rete Windows.

Se non viene specificato un account SNA, SCIEX OS utilizza le credenziali dell'utente attualmente connesso per trasferire i dati nella directory radice di rete. Perché il trasferimento venga effettuato correttamente, l'account deve avere autorizzazioni di scrittura per tutte le cartelle di progetto per le quali sono acquisiti i dati, indipendentemente da quale utente ha inviato il lotto per l'acquisizione.

Processo di trasferimento dei dati

Quando il software SCIEX OS acquisisce i dati in una posizione in rete, per prima cosa scrive ogni campione in una cartella in un'unità locale, quindi lo trasferisce in rete. Quando il corretto trasferimento di tutto il file di dati è confermato, la cartella locale che contiene i dati viene eliminata. Se la rete diventa non disponibile durante questo processo, il software SCIEX OS prova nuovamente ogni 15 minuti fino a quando il trasferimento è completato correttamente.

Per informazioni sull'accesso ai dati durante periodi prolungati di assenza di connettività di rete, fare riferimento alla sezione: [Rimozione di campioni dalle cartelle di trasferimento in rete](#).

Configurazione dell'acquisizione di rete

Una directory radice è la cartella in cui il software SCIEX OS Per garantire un salvataggio sicuro delle informazioni del progetto, creare la directory radice utilizzando il software SCIEX OS. Non creare progetti in File Explorer.

Facoltativamente, quando si creano directory radice su una risorsa di rete, definire **Credentials for Secure Network Account**. È l'account di rete sicuro definito nelle risorse di rete. Fare riferimento alla sezione: [Account di rete sicuro](#).

Per informazioni sulla creazione di progetti e sottoprogetti, fare riferimento al documento: *SCIEX OS Guida per l'utente del software*.

Specificare un account di rete sicura

Se i progetti vengono archiviati in una risorsa di rete, è possibile specificare un account di rete sicuro (SNA) per fare in modo che tutti gli utenti della workstation dispongano dell'accesso necessario alla risorsa di rete.

1. Aprire l'area di lavoro Configuration.
2. Fare clic su **Projects**.
3. Nella sezione **Advanced**, fare clic su **Credentials for Secure Network Account**.
4. Digitare nome utente, password e dominio dell'account di rete sicuro definito nella risorsa di rete.
5. Fare clic su **OK**.

Questa sezione spiega come utilizzare la funzione di auditing. Per informazioni sulle funzioni di auditing di Windows, fare riferimento alla sezione: [Controlli di sistema](#).

Audit trail

Gli eventi controllati sono archiviati negli audit trail. Sono disponibili due tipi di audit trail: workstation e progetto.

Gli audit trail della workstation sono file che archiviano gli eventi controllati per il computer in cui è in esecuzione il software SCIEX OS o Central Administrator Console (CAC). Per un elenco completo degli eventi di audit, fare riferimento alla sezione: [Workstation Audit Trail](#).

Gli audit trail del progetto sono file che archiviano gli eventi di audit per il progetto. Per un elenco completo degli eventi di audit, fare riferimento alla sezione: [Project Audit Trail](#). Nel software SCIEX OS e CAC, l'area di lavoro Audit Trail mostra gli audit trail per i progetti nella directory radice corrente. Gli eventi di audit trail di elaborazione sono contenuti nella mappa di audit trail del progetto e archiviati nella Results Table.

Gli audit trail, associati a file quali i file wiff2 e i file della Results Table, formano record elettronici validi che possono essere utilizzati ai fini della conformità.

Tabella 7-1: Audit Trail

Audit trail	Esempi di eventi registrati	Mappe di audit disponibili memorizzate in	Mappe di audit predefinite
Workstation (SCIEX OS)	<ul style="list-style-type: none">• Cambia in:<ul style="list-style-type: none">• Assegnazione mappa di audit attiva• Tuning dello strumento• Code dei campioni• Sicurezza• Tuning• Dispositivi	<ul style="list-style-type: none">• Cartella C:\ProgramData\SCIEX\ Audit Data	<ul style="list-style-type: none">• No Audit Map

Tabella 7-1: Audit Trail (continua)

Audit trail	Esempi di eventi registrati	Mappe di audit disponibili memorizzate in	Mappe di audit predefinite
Workstation (CAC)	<ul style="list-style-type: none"> • Cambia in: <ul style="list-style-type: none"> • Mappa di audit • Server CAC • Sicurezza • Log utenti 	<ul style="list-style-type: none"> • Cartella C:\ProgramData\SCIEX\ Audit Data 	<ul style="list-style-type: none"> • Silent Audit Map
Progetto (uno per progetto)	<ul style="list-style-type: none"> • Cambia in: <ul style="list-style-type: none"> • Assegnazione mappa di audit attiva (SCIEX OS) • Progetto • Dati • Stampa 	<ul style="list-style-type: none"> • Cartella <project> \Audit Data 	<ul style="list-style-type: none"> • Specificata nella pagina Audit Maps dell'area di lavoro Configuration

Quando Workstation Audit Trail o Project Audit Trail contiene 20.000 record di audit, SCIEX OS e il software CAC archivia automaticamente i record e invia un nuovo audit trail. Per ulteriori informazioni, fare riferimento alla sezione: [Archivi degli audit trail](#).

Mappe di audit

Una mappa di audit è un file che contiene un elenco di tutti gli eventi che è possibile controllare e specifica se per l'evento è necessario un motivo per la modifica o una firma elettronica. Sono disponibili due tipi di mappe di audit: workstation e progetto.

Le mappe di audit della workstation controllano gli eventi controllati in una workstation.

Le mappe di audit del progetto controllano gli eventi controllati per un progetto e sono archiviate nel cartella del progetto.

Nota: La mappa di audit per un progetto può essere modificata nel software SCIEX OS o Central Administrator Console (CAC).

L'utente può creare molte mappe di audit di workstation e progetto, ma solo una di esse può essere in uso in un dato momento per ciascuna workstation e ciascun progetto. La mappa di audit in uso per una workstation o progetto è chiamata mappa di audit attiva.

Se SCIEX OS è installato, la mappa di audit predefinita per tutti i nuovi progetti è No Audit Map. Quando il software CAC è installato, la mappa di audit predefinita per tutti i nuovi

progetti è Silent Audit Map. L'utente può identificare una diversa mappa attiva da usare come predefinita per tutti i nuovi progetti. Fare riferimento alla sezione: [Modifica della mappa di audit attiva per un progetto](#).

Configurazione delle mappe di audit

Prima di iniziare a lavorare con progetti che richiedono auditing, configurare le mappe di audit appropriate alle procedure operative standard. Sono disponibili diverse mappe di audit predefinite quando viene installato il software, tuttavia, potrebbe essere necessario crearne una personalizzata. Assicurarsi che sia disponibile una mappa di audit appropriata per l'audit trail della workstation e per ogni progetto.

Tabella 7-2: Elenco di controllo per la configurazione dell'auditing

Attività	Fare riferimento a
Creare una mappa di audit per l'audit trail workstation.	<ul style="list-style-type: none">• Creazione di una mappa di audit per la workstation.• Modifica di una mappa di audit della workstation.
Applicare la mappa di audit all'audit trail della workstation.	<ul style="list-style-type: none">• Modifica della mappa di audit attiva per una workstation.
Creare una mappa di audit attiva predefinita per nuovi progetti.	<ul style="list-style-type: none">• Creazione di una mappa di audit di progetto.
Configurare la mappa di audit da utilizzare per ogni progetto esistente.	<ul style="list-style-type: none">• Creazione di una mappa di audit di progetto.• Modifica di una mappa di audit del progetto.
Applicare la mappa di audit per ogni progetto esistente.	<ul style="list-style-type: none">• Modifica della mappa di audit attiva per un progetto.

Modelli di mappe di audit installate

Il software include diversi modelli di mappe di audit. Questi modelli non possono essere eliminati o modificati.

Tabella 7-3: Mappe di audit installate

Mappa di audit	Descrizione
Example Audit Map	Gli eventi selezionati vengono controllati. Esclusivamente a scopo illustrativo.
Full Audit Map	Tutti gli eventi vengono controllati. Tutti gli eventi richiedono firme elettroniche e ragioni.

Tabella 7-3: Mappe di audit installate (continua)

Mappa di audit	Descrizione
No Audit Map	Nessun evento viene controllato. Nota: L'evento Change Active Audit Map Assignment viene sempre registrato, anche se non viene usato alcun modello di mappa di audit.
Silent Audit Map	Tutti gli eventi vengono controllati. Per gli eventi non sono richieste né firme elettroniche né ragioni.

Per le descrizioni dei tipi di audit trail e delle relative relazioni alle mappe di audit, fare riferimento alla tabella: [Tabella 7-1](#). Per informazioni sugli eventi registrati negli audit trail, fare riferimento alla sezione: [Record degli audit trail](#).

Per informazioni sul processo di auditing, fare riferimento alla tabella: [Tabella 7-2](#).

Utilizzo di mappe di audit


Il software include diversi modelli di mappe di audit installate. Per le descrizioni dei modelli di mappe di audit, fare riferimento alla sezione: [Modelli di mappe di audit installate](#). Per un elenco di controllo delle operazioni da effettuare per configurare l'auditing, fare riferimento alla sezione: [Configurazione delle mappe di audit](#).

Se un modello di mappa di audit attivo viene eliminato nel software o in File Explorer, il progetto che utilizza quel modello utilizzerà la Silent Audit Map.

Mappe di audit di progetto

Le mappe di audit del progetto controllano l'auditing degli eventi di progetto. Per un elenco degli eventi del progetto che è possibile controllare, fare riferimento alla sezione: [Project Audit Trail](#).

Creazione di una mappa di audit di progetto

1. Aprire l'area di lavoro Configuration.
 2. Fare clic su **Audit Maps**.
 3. Aprire la scheda Projects Templates.
 4. Nel campo **Edit map template**, selezionare un modello da utilizzare come base per la nuova mappa.
 5. Fare clic su **Add Template** ().
- Viene visualizzata la finestra di dialogo Add a Project Audit Map Template.
6. Digitare il nome della nuova mappa, quindi fare clic su **OK**.
 7. Selezionare e configurare gli eventi da registrare effettuando le seguenti operazioni:

Auditing

- a. Selezionare la casella di controllo **Audited** per l'evento.
 - b. (Opzionale) Se è richiesto un motivo, selezionare **Reason Required**.
 - c. (Opzionale) Se è richiesta una firma elettronica, selezionare **E-Sig Required**.
 - d. (Opzionale) Se sono richiesti motivi predefiniti, selezionare **Use Predefined Reason Only** e definire i motivi.
8. Assicurarsi che la casella di controllo **Audited** sia vuota per gli eventi che non verranno controllati.
 9. Fare clic su **Save Template**.
Il sistema chiede se applicare la nuova mappa ai progetti.
 10. Eseguire una delle seguenti operazioni:
 - Per applicare la nuova mappa ai progetti, fare clic su **Yes**, selezionare i progetti che utilizzeranno la nuova mappa, quindi fare clic su **Apply**.
 - Se la nuova mappa non deve essere applicata ai progetti esistenti, fare clic su **No**.
 11. (Opzionale) Per utilizzare questa mappa di audit come predefinita per tutti i nuovi progetti, fare clic su **Use as Default for New Projects**.

Modifica di una mappa di audit del progetto

Nota: Non è possibile modificare i modelli delle mappe di audit installati.

1. Aprire l'area di lavoro Configuration.
2. Fare clic su **Audit Maps**.
3. Aprire la scheda Projects Templates.
4. Nel campo **Edit map template**, selezionare la mappa da modificare.
5. Selezionare e configurare gli eventi da registrare effettuando le seguenti operazioni:
 - a. Selezionare la casella di controllo **Audited** per l'evento.
 - b. (Opzionale) Se è richiesto un motivo, selezionare **Reason Required**.
 - c. (Opzionale) Se è richiesta una firma elettronica, selezionare **E-Sig Required**.
 - d. (Opzionale) Se sono richiesti motivi predefiniti, selezionare **Use Predefined Reason Only** e definire i motivi.
6. Assicurarsi che la casella di controllo **Audited** sia vuota per gli eventi che non verranno controllati.
7. Fare clic su **Save Template**.
Il sistema chiede se applicare la nuova mappa ai progetti.
8. Eseguire una delle seguenti operazioni:
 - Per applicare la nuova mappa ai progetti, fare clic su **Yes**, selezionare i progetti che utilizzeranno la nuova mappa, quindi fare clic su **Apply**.
 - Se la nuova mappa non deve essere applicata ai progetti esistenti, fare clic su **No**.

Modifica della mappa di audit attiva per un progetto

Quando si applica una mappa di audit ad un progetto, questa diventa la mappa di audit attiva. La configurazione di audit nella mappa di audit attiva determina gli eventi che verranno registrati negli audit trail.

1. Aprire l'area di lavoro Configuration.
2. Fare clic su **Audit Maps**.
3. Aprire la scheda Projects Templates.
4. Nel campo **Edit map template**, selezionare la mappa di audit da assegnare al progetto.
5. Fare clic su **Apply to Existing Projects**.
Viene visualizzata la finestra di dialogo Apply Project Audit Map Template.
6. Selezionare le caselle di controllo relative ai progetti che si riferiscono a questa mappa di audit.
7. Fare clic su **Apply**.

Eliminazione di una audit map di progetto

Nota: Non è possibile eliminare i modelli delle mappe di audit installati.

1. Aprire l'area di lavoro Configuration.
2. Fare clic su **Audit Maps**.
3. Aprire la scheda Projects Templates.
4. Nel campo **Edit map template** selezionare la mappa da eliminare.
5. Fare clic su **Delete Template**.
Il sistema richiede conferma.
6. Fare clic su **Yes**.


Mappe di audit della workstation

Le mappe di audit della workstation controllano l'auditing degli eventi della workstation. Per un elenco degli eventi della workstation che è possibile controllare, fare riferimento alla sezione: [Workstation Audit Trail](#).

Creazione di una mappa di audit per la workstation

1. Aprire l'area di lavoro Configuration.
2. Fare clic su **Audit Maps**.
3. Aprire la scheda Workstation Templates.
4. Nel campo **Edit map template**, selezionare un modello da utilizzare come base per la nuova mappa.

Auditing

5. Fare clic su **Add Template** ().
Viene visualizzata la finestra di dialogo Add a Workstation Audit Map Template.
6. Digitare il nome della nuova mappa, quindi fare clic su **OK**.
7. Selezionare e configurare gli eventi da registrare effettuando le seguenti operazioni:
 - a. Selezionare la casella di controllo **Audited** per l'evento.
 - b. (Opzionale) Se è richiesto un motivo, selezionare **Reason Required**.
 - c. (Opzionale) Se è richiesta una firma elettronica, selezionare **E-Sig Required**.
 - d. (Opzionale) Se sono richiesti motivi predefiniti, selezionare **Use Predefined Reason Only** e definire i motivi.
8. Assicurarsi che la casella di controllo **Audited** sia vuota per gli eventi che non verranno controllati.
9. Fare clic su **Save Template**.
10. (Opzionale) Per rendere la presente mappa di audit attiva per la workstation, fare clic su **Apply to the Workstation**.

Modifica di una mappa di audit della workstation

Nota: Non è possibile modificare i modelli delle mappe di audit installati.

1. Aprire l'area di lavoro Configuration.
2. Fare clic su **Audit Maps**.
3. Aprire la scheda Workstation Templates.
4. Nel campo **Edit map template**, selezionare la mappa da modificare.
5. Selezionare e configurare gli eventi da registrare effettuando le seguenti operazioni:
 - a. Selezionare la casella di controllo **Audited** per l'evento.
 - b. (Opzionale) Se è richiesto un motivo, selezionare **Reason Required**.
 - c. (Opzionale) Se è richiesta una firma elettronica, selezionare **E-Sig Required**.
 - d. (Opzionale) Se sono richiesti motivi predefiniti, selezionare **Use Predefined Reason Only** e definire i motivi.
6. Assicurarsi che la casella di controllo **Audited** sia vuota per gli eventi che non verranno controllati.
7. Fare clic su **Save Template**.
8. (Opzionale) Per rendere la presente mappa di audit attiva per la workstation, fare clic su **Apply to the Workstation**.

Modifica della mappa di audit attiva per una workstation

Quando si applica una mappa di audit alla workstation, questa diventa la mappa di audit attiva. La configurazione di audit nella mappa di audit attiva determina gli eventi che verranno registrati negli audit trail.

1. Aprire l'area di lavoro Configuration.
2. Fare clic su **Audit Maps**.
3. Aprire la scheda Workstation Templates.
4. Nel campo **Edit map template**, selezionare la mappa da applicare alla workstation.
5. Fare clic su **Apply to the Workstation**.

Eliminazione di una mappa di audit della workstation

Nota: Non è possibile eliminare i modelli delle mappe di audit installati.

1. Aprire l'area di lavoro Configuration.
2. Fare clic su **Audit Maps**.
3. Aprire la scheda Workstation Templates.
4. Nel campo **Edit map template** selezionare la mappa da eliminare.
5. Fare clic su **Delete Template**.
Il sistema richiede conferma.
6. Fare clic su **Yes**.

Visualizzazione, stampa e ricerca degli audit trail

Questa sezione fornisce informazioni su come visualizzare gli audit trail anche archiviati. Fornisce inoltre le istruzioni per esportare, stampare, cercare e ordinare i record relativi agli stessi.

Visualizzazione di un audit trail

1. Aprire l'area di lavoro Audit Trail.
2. Selezionare l'audit trail da visualizzare:
 - Per visualizzare l'audit trail della stazione di lavoro, fare clic su **Workstation**.
 - Per visualizzare un audit trail di progetto, selezionare il progetto.
3. Per visualizzare i dettagli di un record di audit, selezionare il record.

Ricerca o filtro dei record di audit

1. Aprire l'area di lavoro Audit Trail.

Auditing

2. Selezionare l'audit trail da cercare.
3. Per cercare un record di audit specifico, digitare il testo nel campo **Find in Page**. Tutte le occorrenze del testo specificato nella pagina verranno evidenziate.
4. Per mettere un filtro, seguire i seguenti passaggi:
 - a. Fare clic sull'icona filtro (imbuto).
Viene visualizzata la finestra di dialogo Filter Audit Trail.
 - b. Digitare i criteri di filtro.
 - c. Fare clic su **OK**.

Visualizzazione di un audit trail archiviato

Quando un audit trail contiene 20.000 record, il software SCIEX OS archivia automaticamente i record e inizia un nuovo audit trail. I nomi dei file degli audit trail archiviati indicano il tipo di audit trail, la data e l'ora. Ad esempio, il nome del file per l'audit trail della stazione di lavoro ha il formato WorkstationAuditTrailData-<nome stazione di lavoro>-<YYYY><MMDDHHMMSS>.atds

Questa procedura può essere utilizzata anche per aprire un audit trail per una Results Table.

1. Aprire l'area di lavoro Audit Trail.
2. Fare clic su **Browse**.
3. Navigare e selezionare la mappa di audit archiviata da aprire, quindi fare clic su **OK**.

Nota: Per aprire un audit trail per una Results Table, selezionare il file qsession associato.

Stampa di un audit trail

1. Aprire l'area di lavoro Audit Trail.
2. Selezionare l'audit trail da stampare.
3. Fare clic su **Print**.
Viene visualizzata la finestra di dialogo Print.
4. Selezionare la stampante e fare clic su **OK**.

Esportazione di record degli audit trail

1. Aprire l'area di lavoro Audit Trail.
2. Selezionare l'audit trail da esportare.
3. Fare clic su **Export**.
4. Selezionare il percorso in cui il file esportato verrà archiviato, digitare un **File name** e fare clic su **Save**.
L'audit trail viene salvato come file .csv (valore separato da virgola).

Record degli audit trail

Questa sezione descrive i campi dei record di audit trail.

Gli audit trail della workstation e del progetto sono file crittografati.

Nota: Gli archivi e gli audit trail della workstation sono archiviati nella cartella `Program Data\SCIEX\Audit Data`. Gli archivi e gli audit trail del progetto sono archiviati nella cartella `Audit Data` per il progetto.

Tabella 7-4: Campi record degli eventi

Campo	Descrizione
Timestamp	Data e ora di registrazione.
Event Name	Modulo che ha generato l'evento.
Descrizione	Una descrizione dell'evento.
Reason	Motivo della modifica, come specificato dall'utente, se necessario.
E-signature	Se una firma elettronica è stata fornita.
Full User Name	Il nome dell'utente.
Utente	Nome principale (UPN) dell'utente.
Category	Tipo di evento.

Per gli elenchi di tutti gli eventi registrati nella workstation e negli audit trail del progetto, fare riferimento alle sezioni: [Workstation Audit Trail](#) e [Project Audit Trail](#).

Archivi degli audit trail

I record si accumulano nell'audit trail del progetto e nell'audit trail della workstation e possono creare file grandi, difficili da visualizzare e gestire.

Quando un audit trail raggiunge 20.000 record, viene archiviato. Un record di archiviazione finale viene aggiunto all'audit trail, dopodiché quest'ultimo viene salvato con un nome che indica il tipo di audit trail, la data e l'ora. Viene creato un nuovo audit trail. Il primo record nel nuovo audit trail indica che l'audit trail è stato archiviato e specifica il percorso.

Gli archivi di audit trail della workstation sono archiviati nella cartella `C:\ProgramData\SCIEX\Audit Data`. I nomi file hanno il formato `WorkstationAuditTrailData-<workstation name>-<YYYY><MMDDHHMMSS>.atds`. Ad esempio, `WorkstationAuditTrailData-SWDSXPT158-20190101130401.atds`.

Gli archivi degli audit trail del progetto sono archiviati nella cartella `Audit Data` del progetto.

Accesso ai dati durante le interruzioni di rete

A

Visualizzazione ed elaborazione dati locale

Se si verifica un'interruzione temporanea di rete durante l'acquisizione in rete, è possibile accedere ai dati acquisiti dalla cartella `NetworkBackup` sul computer di acquisizione.

Per evitare di danneggiare i dati, si consiglia di copiare i file di dati nella cartella `NetworkBackup` in un nuovo percorso prima che vengano visualizzati o elaborati e che le copie originali dei file siano conservate nella cartella `NetworkBackup`.

Ogni 15 minuti, il software SCIEX OS determina se il percorso di rete è disponibile. Se lo è, trasferisce i riepiloghi dei dati.

La cartella `NetworkBackup` è contenuta in una directory radice locale, tipicamente `D:\SCIEX OS Data\NetworkBackup`. I file di dati per ogni lotto sono contenuti in una cartella con identificatore unico come nome cartella. Gli indicatori data e ora delle cartelle mostrano la data e l'ora di inizio del lotto e possono essere utilizzati per determinare quale cartella contiene i dati di interesse.

Rimozione di campioni dalle cartelle di trasferimento in rete

Se la connettività di rete viene persa per un periodo di tempo prolungato o se la directory radice di rete è stata modificata, potrebbe essere necessario rimuovere i file di dati dalle cartelle di trasferimento in rete. Consigliamo che questa azione sia eseguita da un amministratore di sistema con capacità tecniche di rete di livello elevato.

1. Aprire l'area di lavoro `Queue`.
2. Interrompere la coda.
3. Annullare tutti i campioni rimanenti nel lotto che contiene i campioni da rimuovere.
4. Chiudere il software SCIEX OS.
5. Arrestare **Clearcore2.Service.exe**.

Suggerimento! Effettuare quest'operazione utilizzando il gestore servizi Windows.

6. Spostare tutti i file e le cartelle nelle cartelle `OutBox` e `NetworkBackup` in attesa del trasferimento alla directory radice non disponibile in un'altra cartella temporanea. Non eliminare le cartelle `OutBox` o `NetworkBackup`.

Nota: La cartella `OutBox` è una cartella nascosta nella directory radice locale, tipicamente `D:\SCIEX OS Data\TempData\Outbox`. Quando i file e le cartelle in `Outbox` non sono più necessari, possono essere rimossi.

ATTENZIONE: Rischio di perdita di dati. Non eliminare i file se i dati del campione bloccato devono essere conservati.

7. Avviare il software SCIEX OS.
Entro 15 minuti, SCIEX OS tenterà di connettersi alla risorsa di rete. Se la connessione avviene correttamente, il trasferimento riprende. Al termine del trasferimento, le cartelle nella cartella `NetworkBackup` sono eliminate.

Eventi di audit

B

Questa sezione elenca gli eventi di audit in SCIEX OS. Elenca inoltre gli eventi di audit corrispondenti nel software Analyst, per gli utenti che eseguono la migrazione dal software Analyst a SCIEX OS.

Project Audit Trail

Ogni progetto dispone di un audit trail del progetto. L'audit trail del progetto è salvato nella cartella `Audit Data` per il progetto. Il nome file dell'audit trail è `ProjectAuditEvents.atds`.

Nota: La mappa di audit predefinita per i nuovi progetti creati nel software Central Administrator Console (CAC) è la **Silent Audit Map**.

Gli eventi di audit trail del progetto vengono mostrati sia nel software CAC sia in SCIEX OS.

Tabella B-1: Eventi di audit trail del progetto

SCIEX OS o CAC	Software Analyst
Area di lavoro Analytics	
Actual Concentration changed	Eventi quantificazione: 'Concentration' è stato modificato
Auto-Processing File saved	—
Barcode ID changed	—
Comparison sample changed in non-targeted workflow	—
Custom columns modified	Eventi quantificazione: 'Custom Title' è stato modificato
Data exploration opened	Eventi progetto: il file di dati è aperto
Data exported	—
Data transferred to LIMS	—
Dilution Factor changed	Eventi quantificazione: 'Dilution Factor' è stato modificato
External calibration changed	—
External calibration exported	—

Tabella B-1: Eventi di audit trail del progetto (continua)

SCIEX OS o CAC	Software Analyst
File saved	Eventi progetto: la Quantitation Results Table è stata creata, la Quantitation Results Table è stata modificata, Eventi quantificazione: la Results Table è stata salvata
Formula column changed	Eventi quantificazione: il nome della formula è stato modificato, il nome della formula è stato aggiunto, la stringa della formula è stata modificata, la colonna della formula è stata rimossa
Integration cleared	—
Integration parameters changed	Eventi quantificazione: il picco di quantificazione è stato integrato
Library search result changed	—
Manual Integration	Eventi quantificazione: il picco di quantificazione è stato integrato
Manual Integration reverted	Eventi quantificazione: il picco di quantificazione è stato ripristinato all'originale
MS/MS selection changed	—
Processing method changed and applied	Eventi quantificazione: il metodo di quantificazione è stato modificato
Report created	Eventi progetto: stampa del documento sulla stampante, fine della stampa del documento sulla stampante
Results Table approved	Eventi quantificazione: il revisore QA ha effettuato l'accesso a una Results Table
Results Table created	Eventi quantificazione: la Results Table è stata creata
Results Table locked	—
Results Table unlocked	—
Sample ID changed	Eventi quantificazione: 'Sample ID' è stato modificato
Sample Name changed	Eventi quantificazione: 'Sample Name' è stato modificato

Eventi di audit

Tabella B-1: Eventi di audit trail del progetto (continua)

SCIEX OS o CAC	Software Analyst
Samples added or removed	Eventi quantificazione: sono stati aggiunti file alla Results Table, sono stati rimossi file dalla Results Table, sono stati aggiunti/rimossi campioni
Sample Type changed	Eventi quantificazione: 'Sample Type' è stato modificato
Std. Addition Actual concentration changed	—
Used column selection changed	Eventi quantificazione: 'Use It' è stato modificato
Window/pane printed	Eventi progetto: stampa del documento sulla stampante, fine della stampa del documento sulla stampante
Pagina Audit Map	
Project Audit Map changed	Eventi progetto: le impostazioni progetto sono state modificate
Project Audit Trail Printed	—
Project Audit Trail Exported	—
Area di lavoro Batch	
Batch information imported from LIMS/ text	—
Print	Eventi progetto: stampa del documento sulla stampante, fine della stampa del documento sulla stampante
Area di lavoro Explorer	
Open Sample(s)	Eventi progetto: il file di dati è aperto
Recalibrate sample(s)	—
Recalibrate sample(s) started	—
Area di lavoro LC Method	
Print	Eventi progetto: stampa del documento sulla stampante, fine della stampa del documento sulla stampante
Area di lavoro MS Method	

Tabella B-1: Eventi di audit trail del progetto (continua)

SCIEX OS o CAC	Software Analyst
Print	Eventi progetto: stampa del documento sulla stampante, fine della stampa del documento sulla stampante
Area di lavoro Queue	
Sample Transferred	—

Workstation Audit Trail

Ogni workstation dispone di un audit trail della workstation. L'audit trail della workstation è salvato nella cartella Program Data\SCIEX\Audit Data. Il nome file dell'audit trail file è in formato: WorkstationAuditTrailData.atds.

Nota: La mappa di audit predefinita per le nuove workstation nel software Central Administrator Console (CAC) è la **Silent Audit Map**.

Gli eventi di audit trail della workstation vengono mostrati sia nel software CAC sia in SCIEX OS.

Tabella B-2: Eventi di audit trail della workstation

SCIEX OS o CAC	Software Analyst
Instrument Tune (SCIEX OS)	
Firmware changed	—
Manual Tuning	Eventi strumento: impostazioni dei parametri di tuning modificate
Automatic Tuning	Eventi strumento: impostazioni dei parametri di tuning modificate
Print Procedure Result in MS Tune	Eventi progetto: stampa del documento sulla stampante, fine della stampa del documento sulla stampante
Hardware Configuration (SCIEX OS)	
Devices Activated	Eventi strumento: il profilo hardware è stato attivato
Devices Deactivated	Eventi strumento: il profilo hardware è stato disattivato
Data File Checksum (SCIEX OS)	
Wiff data file checksum has been changed	—

Eventi di audit

Tabella B-2: Eventi di audit trail della workstation (continua)

SCIEX OS o CAC	Software Analyst
Area di lavoro Explorer (SCIEX OS)	
Open Sample(s)	Eventi progetto: il file di dati è aperto
Recalibrate samples(s)	—
Recalibrate samples(s) started	—
Pagina Audit Map¹	
Workstation Audit Map changed	Eventi strumento: le impostazioni strumento sono state modificate
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	—
Area di lavoro Queue (SCIEX OS)	
Sample moved in Queue	Eventi strumento: campione spostato dalla posizione x alla posizione y del file di lotto
Batch moved in Queue	Eventi strumento: spostamento lotto
Requiring sample	Eventi strumento: riacquisizione campione/i
Sample starts to acquire	—
Print Queue	Eventi progetto: stampa del documento sulla stampante, fine della stampa del documento sulla stampante

¹ Questi eventi sono registrati sia in SCIEX OS sia in CAC.

Tabella B-2: Eventi di audit trail della workstation (continua)

SCIEX OS o CAC	Software Analyst
Sample acquisition has completed	Eventi progetto: il campione è stato aggiunto al file di dati
Automatic reinjections Occurred	—
Automatic injection Occurred	—
Sicurezza¹	
Auto logoff by system	Eventi strumento: utente disconnesso
Forced logoff by another user	Eventi strumento: utente disconnesso
Forced Logoff failed	—
Screen unlock failed	—
Secure Network Account credentials have been changed	Eventi strumento: account di acquisizione modificato
Secure Network Account credentials have been removed	Eventi strumento: account di acquisizione modificato
Secure Network Account credentials have been specified	Eventi strumento: account di acquisizione modificato
Security configuration changed	Eventi strumento: la configurazione di sicurezza è stata modificata, blocco schermo modificato, disconnessione automatica modificata
User added/deleted	Eventi strumento: utente aggiunto, utente eliminato
User has logged in	Eventi strumento: utente connesso
User has logged out	Eventi strumento: utente disconnesso
User has turned off exclusive mode	—
User Login Failed	Eventi strumento: login utente non riuscito
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	Eventi strumento: tipo utente modificato dall'utente
User role deleted	Eventi strumento: tipo utente eliminato

Eventi di audit

Tabella B-2: Eventi di audit trail della workstation (continua)

SCIEX OS o CAC	Software Analyst
User role modified	Eventi strumento: tipo utente modificato
UserLog¹	
Print Event Log	—

Mapping di autorizzazioni tra SCIEX OS e il software Analyst

C

Questa sezione viene fornita per gli utenti che stanno eseguendo la migrazione dal software Analyst a SCIEX OS, per agevolare la migrazione delle impostazioni di sicurezza degli utenti. Mostra le autorizzazioni del software Analyst che corrispondono alle autorizzazioni SCIEX OS.

Tabella C-1: Mapping di autorizzazioni

SCIEX OS	Software Analyst
Area di lavoro Batch	
Submit unlocked methods	—
Open	Lotto: aprire lotti esistenti
Save as	Lotto: creare nuovi lotti, importare, modificare lotti, salvare lotti, sovrascrivere lotti
Submit	Lotto: inviare lotti
Save	Lotti: salvare lotti, sovrascrivere lotti
Save ion reference table	—
Add data sub-folders	—
Configure Decision Rules	—
Area di lavoro Configuration	
General tab	—
General: change regional setting	—
General: full screen mode	—
General: Stop Windows services	—
LIMS Communication tab	—
Audit maps tab	Audit Trail Manager: modificare le impostazioni di audit trail, creare o modificare mappe di audit
Queue tab	—
Queue: instrument idle time	—
Queue: max. number of acquired samples	—
Queue: other queue settings	—

Mapping di autorizzazioni tra SCIEX OS e il software Analyst

Tabella C-1: Mapping di autorizzazioni (continua)

SCIEX OS	Software Analyst
Projects tab	—
Projects: create project	Applicazione Analyst: creare progetti
Projects: apply an audit map template to an existing project	Audit Trail Manager: modificare le impostazioni di audit trail
Projects: create root directory	Applicazione Analyst: creare la directory radice
Project: set current root directory	Applicazione Analyst: impostare la directory radice
Projects: specify network credentials	—
Projects: Enable checksum writing for wiff data creation	—
Projects: clear root directory	—
Devices tab	Configurazione hardware: creare, eliminare, modificare, attivare/disattivare
User management tab	Config. di sicurezza
Force user logoff	Unlock/Logout Application
Area di lavoro Event Log	
Access event log workspace	—
Archive log	—
Area di lavoro Audit Trail	
Access audit trail workspace	Audit Trail Manager: visualizzare dati di audit trail
View active audit map	Audit Trail Manager: visualizzare dati di audit trail
Print/Export audit trail	Audit Trail Manager: visualizzare dati di audit trail
Pannello Data Acquisition	
Start	—
Stop	—
Save	—
Aree di lavoro MS Method e LC Method	
Access method workspace	—

Mapping di autorizzazioni tra SCIEX OS e il software Analyst

Tabella C-1: Mapping di autorizzazioni (continua)

SCIEX OS	Software Analyst
New	Metodo di acquisizione: creare/salvare il metodo di acquisizione
Open	Metodo di acquisizione: aprire il metodo di acquisizione in sola lettura (modalità acquisizione)
Save	Metodo di acquisizione: sovrascrivere metodi di acquisizione, creare/salvare il metodo di acquisizione
Save as	Metodo di acquisizione: sovrascrivere metodi di acquisizione, creare/salvare il metodo di acquisizione
Lock/Unlock method	—
Area di lavoro Queue	
Manage	Coda campioni: riacquisire, eliminare il campione o il lotto, spostare il lotto
Start/Stop	Coda campioni: avviare il campione, arrestare il campione, interrompere il campione, arrestare la coda
Print	Editor modello di report: stampare
Area di lavoro Library	
Access library workspace	Esplora: configurare percorso libreria, configurare opzioni utente libreria, aggiungere record libreria, aggiungere spettro a libreria, modificare record libreria (esclude aggiunta/eliminazione se disabilitati), eliminare spettro MS, eliminare spettro UV, eliminare la struttura, visualizzare libreria, cercare libreria
CAC settings	
Enable Central Administration	—
Area di lavoro MS Tune	
Access MS Tune workspace	—
Advanced MS tuning	Tuning: ottimizzazione strumento, tuning manuale, modificare opzioni di tuning
Advanced troubleshooting	—
Quick status check	Tuning: opzioni strumento

Mapping di autorizzazioni tra SCIEX OS e il software Analyst

Tabella C-1: Mapping di autorizzazioni (continua)

SCIEX OS	Software Analyst
Restore instrument data	Tuning: modificare opzioni di tuning, modificare dati strumenti
Area di lavoro Explorer	
Access explorer workspace	—
Export	Esplora: salvare dati in un file di testo
Print	Editor modello di report: stampare
Options	—
Recalibrate	Tuning: Calibrare da spettro corrente
Area di lavoro Analytics	
New results	Quantificazione: creare nuove results table
Create processing method	Quantificazione: creare metodi di quantificazione
Modify processing method	Quantificazione: modificare metodi esistenti
Allow Export and Create Report of unlocked Results Table	—
Save results for Automation Batch	—
Change default quantitation method integration algorithm	Quantificazione: modificare le opzioni metodo predefiniti
Change default quantitation method integration parameters	Quantificazione: modificare le opzioni metodo predefiniti
Enable project modified peak warning	—
Add samples	Quantificazione: aggiungere e rimuovere campioni dalla results table
Remove selected samples	Quantificazione: aggiungere e rimuovere campioni dalla results table
Export, import or remove external calibration	—
Modify sample name	Quantificazione: modificare nome campione
Modify sample type	Quantificazione: modificare tipo campione
Modify sample ID	Quantificazione: modificare ID campione
Modify actual concentration	Quantificazione: modificare concentrazione di analita

Mapping di autorizzazioni tra SCIEX OS e il software Analyst

Tabella C-1: Mapping di autorizzazioni (continua)

SCIEX OS	Software Analyst
Modify dilution factor	Quantificazione: modificare fattore di diluizione
Modify comments fields	Quantificazione: modificare commento campione
Enable manual integration	Quantificazione: integrare manualmente
Set peak to not found	—
Include or exclude a peak from the results table	Quantificazione: escludere standard dalla calibrazione
Regression options	Quantificazione: modificare i parametri di regressione
Modify the results table integration parameters for a single chromatogram	Quantificazione: modificare i parametri "semplici" in peak review, modificare i parametri "avanzati" in peak review
Modify quantitation method for results table component	Quantificazione: modificare il metodo delle Results Table
Create metric plot new settings	Quantificazione: modificare o creare impostazioni diagrammi metrici
Add custom columns	Quantificazione: creare o modificare colonne della formula
Set peak review title format	—
Remove custom column	Quantificazione: creare o modificare colonne della formula
Results table display settings	Quantificazione: modificare la precisione delle colonne della results table, modificare la visibilità delle colonne della results table, modificare le impostazioni della results table
Lock results table	—
Unlock results table	—
Mark results file as reviewed and save	—
Modify report template	Editor modello di report: creare/modificare modelli di report
Transfer results to LIMS	—
Modify barcode column	—
Change comparison sample assignment	—
Add the MSMS spectra to library	Esplora, aggiungere spettro al record libreria

Mapping di autorizzazioni tra SCIEX OS e il software Analyst

Tabella C-1: Mapping di autorizzazioni (continua)

SCIEX OS	Software Analyst
Project default settings	Quantificazione: modificare le impostazioni globali (predefinite)
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	Quantificazione: creare gruppi di analiti, modificare gruppi di analiti
Browse for files	—
Enable standard addition	—
Set Manual Integration Percentage Rule	Quantificazione: abilitare o disabilitare regola percentuale in integrazione manuale

Si consiglia agli utenti di utilizzare i checksum dei file di dati per i file wiff. La funzione checksum è un controllo a ridondanza ciclica per verificare l'integrità del file di dati.

Se la funzione Data File Checksum è abilitata, quando l'utente crea un file di dati (wiff), il software genera un valore di checksum utilizzando un algoritmo basato sull'algoritmo di crittografia pubblica MD5 e salva il valore nel file. Quando viene verificato il checksum, il software calcola il checksum e confronta il checksum calcolato con il checksum memorizzato nel file.

Il confronto tra checksum può portare a tre diversi risultati:

- Se i valori corrispondono, il checksum è valido.
- Se i valori non corrispondono, il checksum non è valido. Un checksum non valido indica che il file è stato modificato al di fuori del software oppure che il file è stato salvato con il calcolo del checksum abilitato e il checksum è diverso dal checksum originale.
- Se il file non dispone di un valore di checksum memorizzato, il checksum non viene trovato. Un file non ha un valore di checksum memorizzato in quanto il file è stato salvato quando l'opzione Data File Checksum era disabilitata.

Nota: L'utente può verificare il checksum utilizzando il software Analyst. Fare riferimento alla documentazione per il software Analyst.

Abilitazione o disabilitazione dell'opzione Data File Checksum

1. Aprire l'area di lavoro Configuration.
2. Fare clic su **Projects**.
3. Se richiesto, espandere **Data File Security**.
4. Per abilitare la funzione Data File Checksum, selezionare la casella di controllo **Enable checksum writing for wiff data creation**. Per disabilitare la funzione, deselezionare questa casella di controllo.

Contatti

Formazione dei clienti

- In Nord America: NA.CustomerTraining@sciex.com
- In Europa: Europe.CustomerTraining@sciex.com
- Al di fuori dell'Unione Europea e del Nord America, visitare sciex.com/education per trovare le informazioni di contatto.

Centro di istruzione online

- [SCIEX Now Learning Hub](#)

Assistenza SCIEX

SCIEX e i suoi rappresentanti si affidano a uno staff di tecnici di manutenzione e assistenza formati e qualificati, presenti in tutto il mondo. Saranno felici di rispondere a domande sul sistema o su eventuali problemi tecnici che potrebbero sorgere. Per ulteriori informazioni, visitare il sito web SCIEX all'indirizzo sciex.com oppure è possibile contattarci in uno dei seguenti modi:

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

Sicurezza informatica

Per le ultime indicazioni sulla sicurezza informatica per i prodotti SCIEX, visitare il sito sciex.com/productsecurity.

Documentazione

Questa versione sostituisce tutte le versioni precedenti del documento.

Per visualizzare il documento in formato elettronico, è necessario che sia installato Adobe Acrobat Reader. Per scaricare la versione più recente, visitare il sito Web <https://get.adobe.com/reader>.

Per reperire la documentazione del software del prodotto, fare riferimento alle note di rilascio o alla guida all'installazione del software fornita con il software.

Per reperire la documentazione dell'hardware del prodotto, fare riferimento al DVD della documentazione del sistema o del componente.

Le versioni più recenti della documentazione sono disponibili sul sito Web SCIEX, all'indirizzo sciex.com/customer-documents.

Nota: per richiedere una versione stampata gratuita del presente documento, contattare sciex.com/contact-us.
