SCIEX
The Power of Precision

Software SCIEX OS

Guida del direttore del laboratorio

RUO-IDV-05-7370-IT-L

Agosto 2023

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.

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

Sommario

Introduzione 1

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 descrive il modo in cui i componenti di controllo e auditing degli accessi nel software SCIEX OS funzionano congiuntamente ai componenti di controllo e auditing di Windows. Descrive inoltre come configurare la sicurezza di Windows prima dell'installazione del software 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.

SCIEX OS e protezione Windows: funzionamento combinato

Il software SCIEX OS e Windows New Technology File System (NTFS) 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.

Il software SCIEX OS offre le seguenti modalità di accesso sicuro al sistema:

- 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 al software SCIEX OS.

Audit trail nel software SCIEX OS e in Windows

Le funzionalità di auditing nel software SCIEX OS, insieme ai componenti di auditing 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 nel software SCIEX OS.
- Creazione e modifica di informazioni sui campioni, parametri di integrazione picchi e metodo di trattamento incorporato in una Tabella dei risultati.

Per un elenco completo di eventi di audit, fare riferimento alla sezione: Eventi di audit.

Il software SCIEX OS utilizza il log 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 log 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

Il software SCIEX OS contiene i controlli tecnici per supportare la conformità 21 CFR Parte 11 con l'implementazione di:

- Sicurezza delle modalità Mixed e Integrated 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.

Il software SCIEX OS è progettato per essere usato come parte del sistema conforme alle norme 21 CFR Parte 11 e può essere configurato per supportare la conformità alle norme 21 CFR Parte 11. Il fatto che l'uso del software SCIEX OS sia conforme o meno alle norme 21 CFR Parte 11 dipende dall'uso della licenza per SCIEX OS CFR e dalla configurazione del software SCIEX OS. Devono inoltre essere presenti nel laboratorio i criteri e le procedure necessari e devono essere soddisfatti i requisiti di formazione relativi.

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

Nota: Non lasciare il software Instrument Settings Converter su un sistema convalidato. È stato progettato per il trasferimento iniziale delle impostazioni strumento da Analyst al software SCIEX OS. Assicurarsi di rimuovere il software Instrument Settings 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

Questa sezione fornisce linee guida per la configurazione di Windows:

- Attenersi a queste linee guida per gli account e le password di Windows:
  - 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.
  - 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**, **Amministratore** o **demo**.
- Assicurarsi che l'amministratore del software SCIEX OS possa modificare le autorizzazioni sui file nella 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 assicurarsi che tutti gli utenti dispongano dell'accesso alle risorse per l'acquisizione di rete, chiedere all'amministratore di rete di aggiungere 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.

Nota: Si consiglia di importare i file libreria da un'unità locale.

Nota: Per informazioni sulle autorizzazioni di Windows richieste per i diversi ruoli utente, fare riferimento alla sezione: Autorizzazioni di Windows.

Utenti e gruppi

SCIEX OS utilizza i nomi utente e le password registrati nel database di sicurezza di Primary Domain Controller 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 al software SCIEX OS.

Supporto per Active Directory

Quando si aggiungono utenti nell'area di lavoro Configurazione di SCIEX OS, specificare gli account utente in 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

Nel software 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 del software

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.

Nota: Per evitare i problemi di autorizzazioni, si consiglia di importare i file libreria da un'unità locale.

Nota: Per informazioni sulle autorizzazioni di Windows richieste per i diversi ruoli utente, fare riferimento alla sezione: Autorizzazioni di Windows.

Per informazioni sulle autorizzazioni su file e cartelle nel 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 log eventi.

Log 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 log eventi come descritto di seguito:

- Configurare un log 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.

Licenze elettroniche 3

Per il software SCIEX OS, le licenze elettroniche possono essere vincolate al nodo o basate su server.

Per il software Central Administrator Console (CAC), sono disponibili solo licenze 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 Configurazione fare clic su **Licenze** nella finestra del software SCIEX OS.

Nota: Assicurarsi di effettuare il rinnovo della licenza prima della scadenza. La licenza per il software CAC è annuale.

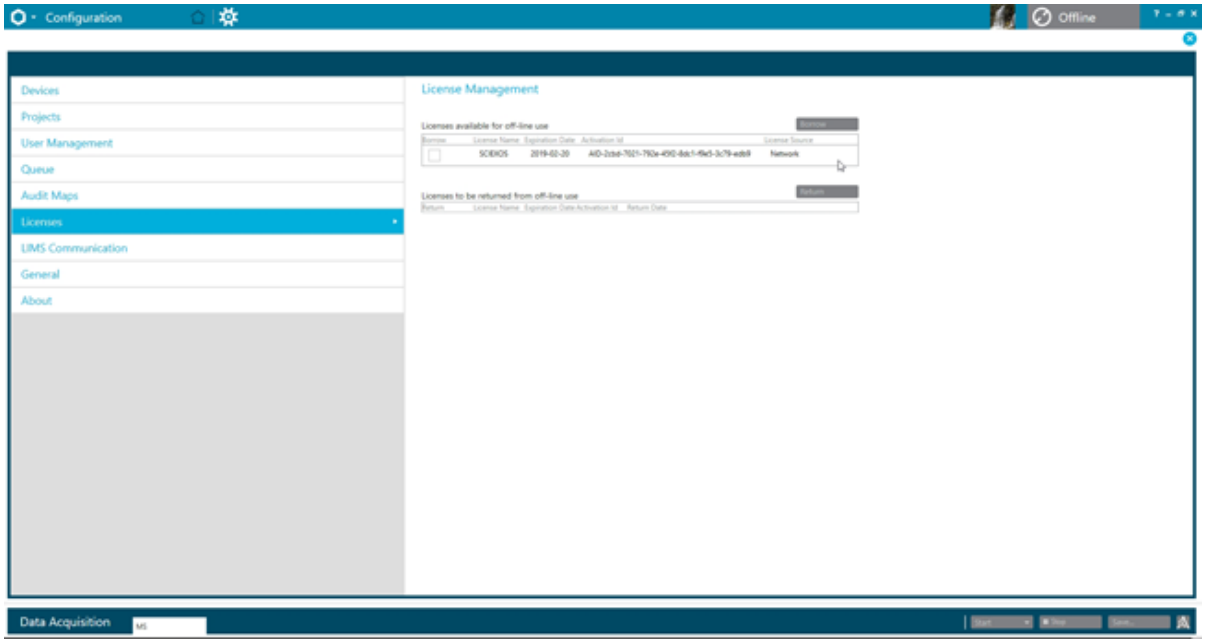
Prestito di una licenza elettronica basata su server

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 Configurazione.
2. Fare clic su **Licenze**.
   La seguente tabella Licenze disponibili per l'uso offline mostra tutte le licenze disponibili per il prestito.

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



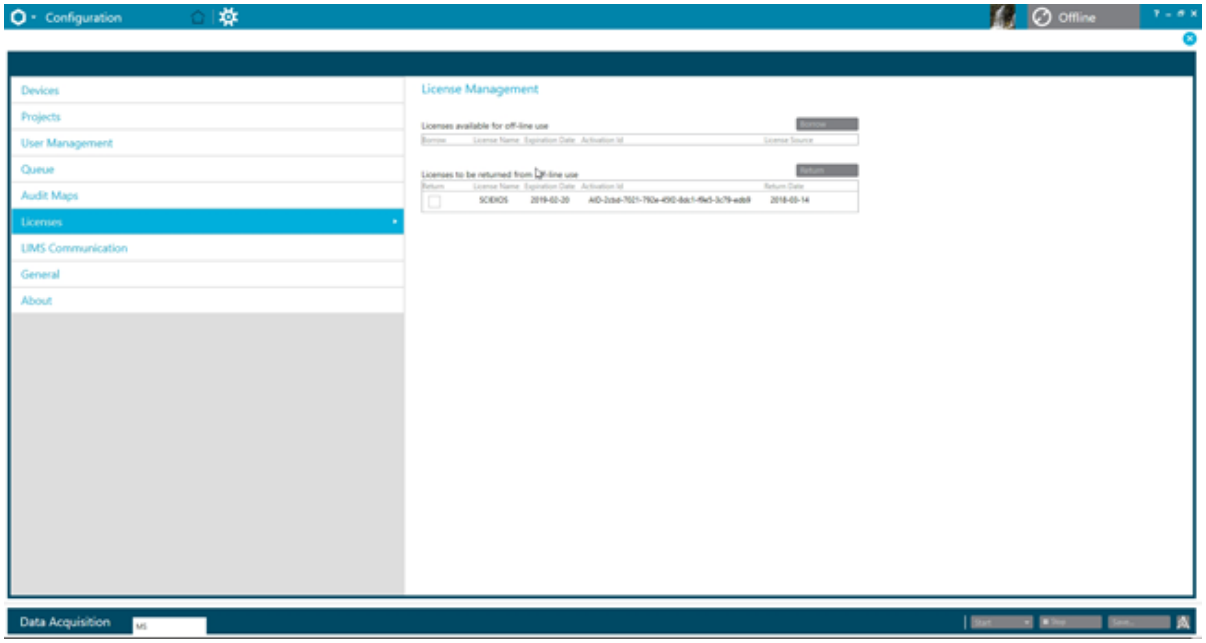
3. Selezionare la licenza da prendere in prestito e fare clic su **Prendi in prestito**.

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 Configurazione.
2. Fare clic su **Licenze**.
   La tabella Licenze da restituire dall'uso offline mostra tutte le licenze idonee alla restituzione, ovvero tutte le licenze prese in prestito da questo computer.

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



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

Controllo dell'accesso 4

In questa sezione viene descritto come controllare l'accesso al software SCIEX OS. Per controllare l'accesso al software, 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 il software SCIEX OS.
- Aggiungere ed eliminare utenti e ruoli.
- Configurare l'accesso ai progetti e ai file di progetto nella directory radice.

Questa procedura fornisce istruzioni per l'amministrazione locale del software SCIEX OS. Per l'amministrazione centralizzata del software 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

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

Configurazione della protezione ai seguenti livelli:

- Autenticazione Windows: accesso al computer.
- Autenticazione Windows: accesso a file e cartelle.
- Autenticazione del software SCIEX OS: possibilità di aprire SCIEX OS.
- Autorizzazione del software 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 il software SCIEX OS.	Fare riferimento al documento: *Guida all'installazione del software SCIEX OS*.
Configurare l'accesso al software SCIEX OS.	Fare riferimento alla sezione: Configurazione dell'accesso al software 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
Windows Security	
Configurare utenti e gruppi (autenticazione).	Sì
Abilitare l'auditing di Windows e di file e directory.	Sì
Impostare le autorizzazioni file (autorizzazione).	Sì
SCIEX OS Software Installation	
Installare il software SCIEX OS.	Sì
Aprire il Visualizzatore eventi per ispezionare l'installazione.	Sì
Software Security	
Selezionare la modalità di sicurezza.	Sì
Configurare utenti e ruoli nel software 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 del software SCIEX OS

Prima di installare il software 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 di audit personalizzate e assegnare una mappa di audit diversa nell'area di lavoro Configurazione.

Configurazione della modalità di protezione

Questa sezione descrive le opzioni Modalità sicurezza che si trovano nella pagina Gestione utenti nell'area di lavoro Configurazione.

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

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 SCIEX OS. 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 e trattamento continuano. La disconnessione automatica non viene effettuata se è in corso il trattamento o se la Tabella dei risultati non è stata salvata. Quando l'utente viene disconnesso in modo forzato, ogni trattamento 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 sicurezza non può essere gestita con il software SCIEX OS.

Selezione della modalità di protezione

1. Aprire l'area di lavoro Configurazione.
2. Fare clic su **Gestione utenti**.
3. Fare clic sulla scheda **Modalità sicurezza**.
4. Selezionare **Modalità integrata** o **Modalità mista**. Fare riferimento alla sezione: Configurazione della modalità di protezione.
5. Fare clic su **Salva**.
   Viene visualizzata una finestra di dialogo di conferma.
6. Fare clic su **OK**.

Configurazione delle opzioni di protezione della workstation (Mixed Mode)

Procedure preliminari
• 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 Configurazione.
2. Fare clic su **Gestione utenti**.
3. Aprire la scheda Modalità sicurezza.
4. Per configurare la funzione Screen Lock, attenersi alla procedura seguente:
   a. Selezionare **Blocco schermo**.
   b. Nel campo **Attendere**, 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 **Disconnessione automatica**.
   b. Nel campo **Attendere**, 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 trattamento si interrompe. L'acquisizione, tuttavia, continua.
6. Fare clic su **Salva**.
   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 Configurazione.
2. Fare clic su **Gestione utenti**.
3. Aprire la scheda Modalità sicurezza.
4. Selezionare la casella di controllo **Invia messaggi e-mail dopo** 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 **Invia messaggi e-mail dopo**.
5. Nel campo **Server SMTP**, 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 **Numero porta**, digitare il numero della porta aperta.
   Fare clic su **Applica valori predefiniti** per inserire il numero di porta predefinito, 25.
7. Nel campo **A**, digitare l'indirizzo e-mail a cui verrà inviato il messaggio. Ad esempio: nomeutente@dominio.com.
8. Nel campo **Da**, digitare l'indirizzo e-mail che comparirà nel campo **Da** del messaggio.
9. Nel campo **Oggetto**, digitare l'oggetto del messaggio.
10. Nel campo **Messaggio**, digitare il testo che verrà incluso nel corpo del messaggio.
11. Fare clic su **Salva**.
    Viene visualizzata una finestra di dialogo di conferma.
12. Fare clic su **OK**.
13. Per controllare la configurazione, fare clic su **Invia e-mail di prova**.

Configurazione dell'accesso al software 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 dei criteri gruppo con l'amministratore di Active Directory come parte di una distribuzione completa del software SCIEX OS.

Autorizzazioni SCIEX OS

Figura 4-1: Pagina User Management

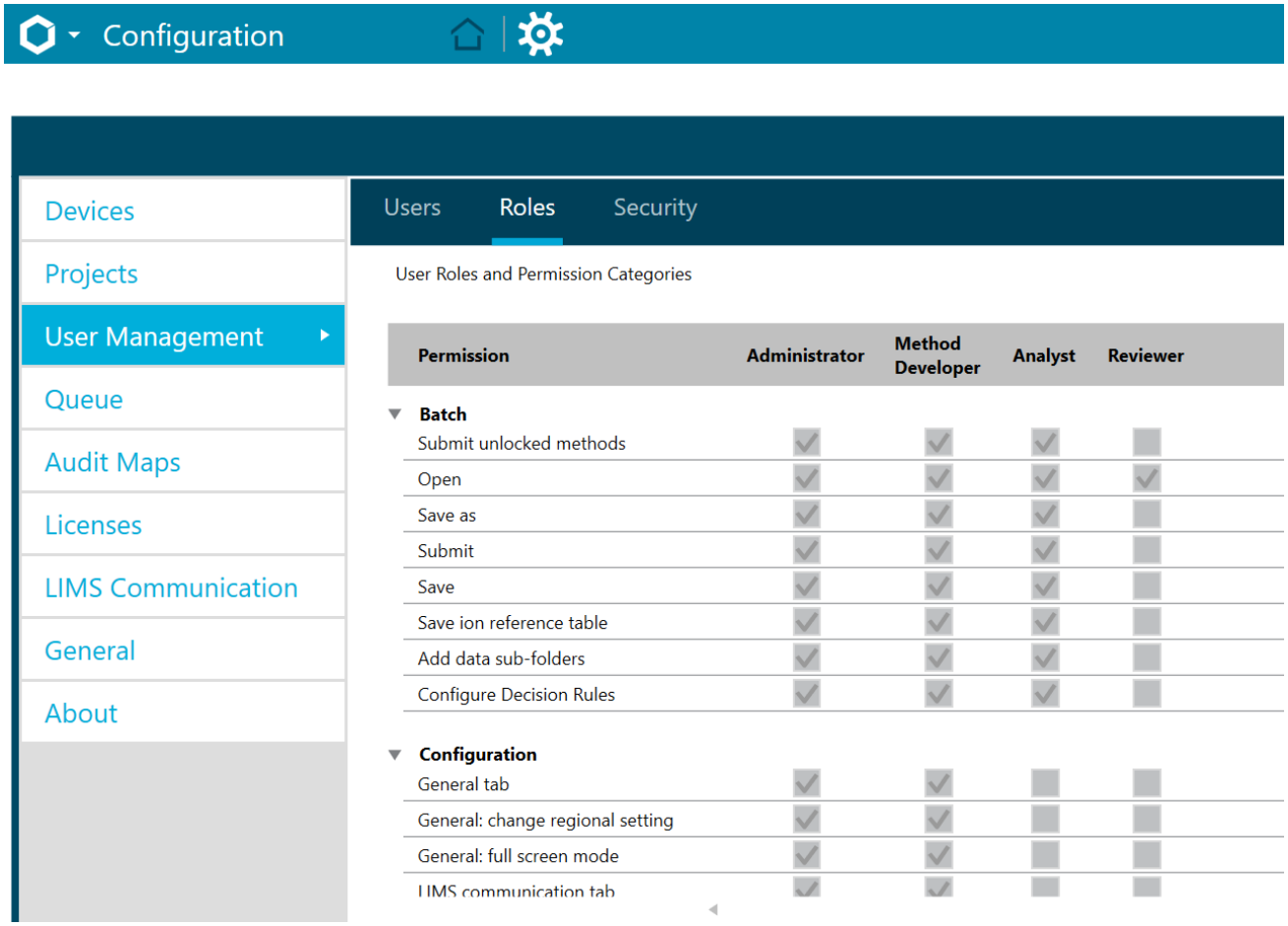


Tabella 4-3: Autorizzazioni

Autorizzazione	Descrizione
Lotto	
Invia metodi sbloccati	Consente agli utenti di inviare lotti che contengono metodi non bloccati.
Apri	Consente agli utenti di aprire lotti esistenti.
Salva con nome	Consente agli utenti di salvare lotti con un nuovo nome.
Invia	Consente agli utenti di inviare lotti.
Salva	Consente agli utenti di salvare un lotto e sovrascrivere il contenuto esistente.
Salva tabella di riferimento ionica	Consente agli utenti di modificare la tabella di riferimento di ionizzazione.

Tabella 4-3: Autorizzazioni (continua)

Autorizzazione	Descrizione
Aggiungi sottocartelle dati	Consente agli utenti di creare sottocartelle per l'archiviazione dei dati.
Configura regole di decisione	Consente agli utenti aggiungere e modificare le regole di decisione.
Configurazione	
Scheda Generale	Consente agli utenti di aprire la pagina Generale nell'area di lavoro Configurazione.
Generale: modifica impostazione regionale	Consente agli utenti di applicare le impostazioni internazionali del sistema attivo al software SCIEX OS.
Generale: modalità schermo intero	Consente agli utenti di attivare e disattivare la modalità a schermo intero.
Generale: arresta i servizi Windows	Consente agli utenti di abilitare o disabilitare l'opzione **Impostazioni Windows**.
Scheda Comunicazione LIMS	Consente agli utenti di aprire la pagina Comunicazione LIMS nell'area di lavoro Configurazione.
Scheda mappe di audit	Consente agli utenti di aprire la pagina Mappe di audit nell'area di lavoro Configurazione.
Scheda Coda	Consente agli utenti di aprire la pagina Coda nell'area di lavoro Configurazione.
Coda: tempo inattività strumento	Consente agli utenti di impostare il tempo di inattività dello strumento.
Coda: numero max. di campioni acquisiti	Consente agli utenti di impostare il numero massimo consentito di campioni acquisiti.
Coda: altre impostazioni coda	Consente agli utenti di configurare altre impostazioni della coda.
Scheda Progetti	Consente agli utenti di aprire la pagina Progetti nell'area di lavoro Configurazione.
Progetti: crea progetto	Consente agli utenti di creare progetti.
Progetti: applica un modello mappa di audit a un progetto esistente	Consente agli utenti di applicare una mappa di audit a un progetto.
Progetti: crea directory radice	Consente agli utenti di creare una directory radice per l'archiviazione dei progetti.
Progetti: imposta directory radice corrente	Consente agli utenti di modificare la directory radice per un progetto.

Tabella 4-3: Autorizzazioni (continua)

Autorizzazione	Descrizione
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.
Progetti: abilita scrittura checksum per creazione dati wiff	Consente agli utenti di configurare il software per scrivere checksum nei file di dati `wiff`.
Progetti: cancella directory radice	Consente agli utenti di eliminare una directory radice dall'elenco.
Scheda Dispositivi	Consente agli utenti di aprire la pagina Dispositivi nell'area di lavoro Configurazione.
Scheda Gestione utenti	Consente agli utenti di aprire la pagina Gestione utenti nell'area di lavoro Configurazione.
Forza disconnessione utente	Consente agli utenti di imporre la disconnessione di un utente connesso al software SCIEX OS.
Scheda CAC [1]	Consente agli utenti di aprire la pagina CAC nell'area di lavoro Configurazione.
Scheda Modelli di stampa	Consente agli utenti di aprire la scheda Modelli di stampa nell'area di lavoro Configurazione.
Modelli di stampa: crea e modifica modelli di stampa	Consente agli utenti di creare nuovi modelli di stampa o modificare i modelli di stampa esistenti.
Modelli di stampa: imposta modello di stampa predefinito	Consente agli utenti di impostare come predefinito il modello di stampa attivo per il progetto attivo.
Modelli di stampa: applica il modello corrente a tutti i progetti nella directory radice	Consente agli utenti di aggiungere il modello di stampa all'elenco dei modelli di stampa disponibili per i progetti selezionati in una directory radice selezionata.
Log eventi	
Accedi all'area di lavoro log eventi	Consente agli utenti di aprire l'area di lavoro Log eventi.
Archivia log	Consente agli utenti di archiviare i log nell'area di lavoro Log eventi.
Audit trail	

[1] Nella versione 3.1, l'autorizzazione **Abilita amministrazione centrale** è stata rinominata in **CAC**. La pagina CAC nell'area di lavoro Configurazione consente di configurare l'amministrazione centrale del software SCIEX OS.

Tabella 4-3: Autorizzazioni (continua)

Autorizzazione	Descrizione
Accedi all'area di lavoro audit trail	Consente agli utenti di aprire l'area di lavoro Audit trail.
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.
Stampa/Esporta audit trail	Consente agli utenti di stampare o esportare l'audit trail.
Pannello di acquisizione dati	
Inizio	Consente agli utenti di avviare l'acquisizione nel riquadro Acquisizione dati.
Interrompi	Consente agli utenti di arrestare l'acquisizione nel riquadro Acquisizione dati.
Salva	Consente agli utenti di salvare i dati acquisiti con un nome file diverso nel riquadro Acquisizione dati.
Metodo MS e LC	
Accedi all'area di lavoro metodo	Consente agli utenti di aprire le aree di lavoro Metodo MS e Metodo LC.
Nuovo	Consente agli utenti di creare metodi MS e LC.
Apri	Consente agli utenti di aprire i metodi MS e LC.
Salva	Consente agli utenti di salvare un metodo e sovrascrivere il contenuto esistente.
Salva con nome	Consente agli utenti di salvare metodi con un nuovo nome.
Blocca/Sblocca metodo	Consente di bloccare i metodi, per impedirne la modifica oppure di sbloccarli.
Coda	
Gestisci	Consente agli utenti di aprire l'area di lavoro Coda.
Avvia/Arresta	Consente agli utenti di avviare o interrompere la coda.
Stampa	Consente agli utenti di stampare la coda.
Modifica campione	Consente agli utenti di modificare il nome o il file di dati di un campione.
Libreria	
Accedi all'area di lavoro libreria	Consente agli utenti di aprire l'area di lavoro Libreria. Non applicabile al flusso di lavoro di quantificazione.
MS Tune	

Tabella 4-3: Autorizzazioni (continua)

Autorizzazione	Descrizione
Accedi all'area di lavoro MS Tune	Consente agli utenti di aprire l'area di lavoro MS Tune.
Tuning MS avanzato	Sistemi X500 QTOF e ZenoTOF 7600: consente agli utenti di accedere alle opzioni di tuning avanzate, tra cui **Ottimizzazione rilevatore**, **Tuning TOF modalità positiva**, **Tuning TOF modalità negativa**, **Tuning unità Q1 modalità positiva**, **Tuning unità Q1 modalità negativa**, **Tuning Q1 alto modalità positiva** e **Tuning Q1 alto modalità negativa**.
Risoluzione dei problemi avanzata	Consente agli utenti di aprire la finestra di dialogo Risoluzione dei problemi avanzata.
Controllo stato rapido	Sistemi X500 QTOF e ZenoTOF 7600: consente agli utenti di eseguire **Controllo stato rapido modalità positiva** e **Controllo stato rapido modalità negativa**.
Ripristina dati strumento	Consente agli utenti di ripristinare la regolazione delle impostazioni salvate in precedenza.
Explorer	
Accedi all'area di lavoro Explorer	Consente agli utenti di aprire l'area di lavoro Explorer.
Esporta	Consente agli utenti di esportare dati dall'area di lavoro Explorer.
Stampa	Consente agli utenti di stampare dati nell'area di lavoro Explorer.
Opzioni	Consente agli utenti di modificare le opzioni per l'area di lavoro Explorer.
Ricalibra	Consente agli utenti di ricalibrare campioni e spettri nell'area di lavoro Explorer. Non applicabile al flusso di lavoro di quantificazione.
Analisi	
Nuovi risultati	Consente agli utenti di creare Tabelle dei risultati.
Crea metodo di elaborazione	Consente agli utenti di creare metodi di trattamento.
Modifica metodo di elaborazione	Consente agli utenti di modificare i metodi di trattamento.

Tabella 4-3: Autorizzazioni (continua)

Autorizzazione	Descrizione
Consenti l'esportazione e la creazione del report della tabella dei risultati sbloccata	Consente agli utenti di esportare o generare un report da una Tabella dei risultati o da una tabella delle statistiche, se la Tabella dei risultati non è bloccata.
Salva risultati per lotto automazione	Consente di salvare le Tabelle dei risultati create automaticamente nell'area di lavoro Lotto. Questa autorizzazione è necessaria per il trattamento automatico durante l'acquisizione.
Modifica algoritmo di integrazione metodo di quantificazione predefinito	Consente agli utenti di modificare l'algoritmo di integrazione nelle impostazioni predefinite di progetto.
Modifica parametri di integrazione metodo di quantificazione predefinito	Consente agli utenti di modificare i parametri di integrazione nelle impostazioni predefinite di progetto.
Abilita avviso picco modificato progetto	Consente agli utenti di abilitare la proprietà dell'avviso di picco modificato per un progetto.
Aggiungi campioni	Consente agli utenti di aggiungere campioni in una Tabella dei risultati.
Rimuovi campioni selezionati	Consente agli utenti di rimuovere campioni da una Tabella dei risultati.
Esporta, importa o rimuovi calibrazione esterna	Consente agli utenti di esportare, importare o rimuovere le calibrazioni esterne.
Modifica nome campione	Consente agi utenti di modificare il nome del campione nella Tabella dei risultati.
Modifica tipo di campione	Consente agli utenti di modificare il tipo di campione nella Tabella dei risultati. I tipi di campioni validi sono: standard, controllo qualità (QC) e sconosciuto.
Modifica ID campione	Consente agli utenti di modificare l'ID del campione nella Tabella dei risultati.
Modifica concentrazione effettiva	Consente agli utenti di modificare la concentrazione effettiva dei campioni standard e QC nella Tabella dei risultati.
Modifica fattore di diluizione	Consente agli utenti di modificare il fattore di diluizione nella Tabella dei risultati.

Tabella 4-3: Autorizzazioni (continua)

Autorizzazione	Descrizione
Modifica campi commento	Consente agli utenti di modificare i campi dei commenti seguenti: • **Commento componente** • **Commento IS** • **Commento picco IS** • **Commento picco** • **Commento campione**
Abilita integrazione manuale	Consente agli utenti di eseguire l'integrazione manuale.
Imposta picco su non trovato	Consente agli utenti di impostare un picco su **Non trovato**.
Includi o escludi un picco dalla tabella dei risultati	Consente agli utenti di includere o escludere i picchi nella Tabella dei risultati.
Opzioni di regressione	Consente agli utenti di modificare le opzioni di regressione nel riquadro Curva di calibrazione.
Modifica parametri di integrazione tabella dei risultati per un singolo cromatogramma	Consente agli utenti di modificare i parametri di integrazione per un unico cromatogramma nel riquadro di verifica dei picchi.
Modifica metodo di quantificazione per componente tabella dei risultati	Consente agli utenti di selezionare un metodo di trattamento diverso per un componente nel riquadro di verifica dei picchi con l'opzione **Aggiorna metodo di trattamento per il componente**.
Crea nuove impostazioni tracciato metrico	Consente agli utenti di creare nuovi tracciati metrici e modificare le impostazioni.
Aggiungi colonne personalizzate	Consente agli utenti di aggiungere delle colonne personalizzate in una Tabella dei risultati.
Imposta formato titolo verifica picco	Consente agli utenti di modificare il titolo della verifica del picco.
Rimuovi colonna personalizzata	Consente agli utenti di rimuovere delle colonne personalizzate da una Tabella dei risultati.
Impostazioni di visualizzazione tabella dei risultati	Consente agli utenti di personalizzare le colonne visualizzate nella Tabella dei risultati.
Blocca tabella dei risultati	Consente agli utenti di bloccare una Tabella dei risultati per impedirne la modifica.

Tabella 4-3: Autorizzazioni (continua)

Autorizzazione	Descrizione
Sblocca tabella dei risultati	Consente agli utenti di sbloccare una Tabella dei risultati per consentire di apportare modifiche.
Contrassegna file dei risultati come rivisto e salva	Consente agli utenti di contrassegnare una Tabella dei risultati come rivista e salvarla.
Modifica modello report	Consente agli utenti di modificare i modelli di report.
Trasferisci risultati a LIMS	Consente agli utenti caricare risultati in un sistema LIMS (Laboratory Information Management System).
Modifica colonna codice a barre	Consente agli utenti di modificare la colonna **Codice a barre** in una Tabella dei risultati.
Modifica assegnazione campione di confronto	Consente agli utenti di modificare il campione di confronto specificato nella colonna **Confronto** della Tabella dei risultati.
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.
Impostazioni predefinite progetto	Consente agli utenti di modificare le impostazioni predefinite di trattamento quantitativo e qualitativo del progetto.
Crea report in tutti i formati	Consente agli utenti di creare report in tutti i formati. Gli utenti che non hanno questa autorizzazione possono generare solo report in formato PDF.
Modifica parametri criteri di segnalazione	Consente agli utenti di modificare i parametri di segnalazione in un metodo di trattamento.
Modifica parametro di rimozione automatica anomalie	Consente agli utenti di modificare i parametri per la rimozione automatica dei valori anomali.
Abilita rimozione automatica anomalie	Consente agli utenti di modificare il metodo di trattamento per attivare la funzione di rimozione automatica dei valori anomali.
Aggiorna metodo di trattamento tramite FF/LS	Consente agli utenti di utilizzare Formula Finder e Library Search per aggiornare i metodi di trattamento. Non applicabile al flusso di lavoro di quantificazione.
Aggiorna risultati tramite FF/LS	Consente agli utenti di utilizzare Formula Finder e Library Search per aggiornare i risultati. Non applicabile al flusso di lavoro di quantificazione.
Abilita funzionalità di raggruppamento per addotti	Consente agli utenti di aggiornare il metodo di trattamento per utilizzare la funzione di raggruppamento per addotti.

Tabella 4-3: Autorizzazioni (continua)

Autorizzazione	Descrizione
Cerca file	Consente agli utenti di navigare al di fuori della cartella dati locale.
Abilita aggiunta standard	Consente agli utenti di aggiornare il metodo di trattamento per attivare la funzione di aggiunta standard.
Imposta regola percentuale di integrazione manuale	Consente agli utenti di modificare il parametro **% integrazione manuale**.
Modifica peso/volume	Consente agli utenti di modificare il campo **Peso/Volume**.

Informazioni su utenti e ruoli

Nel software SCIEX OS, l'amministratore può aggiungere utenti e gruppi di Windows al database User Management. 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 preimpostati, descritti nella tabella seguente, o a ruoli personalizzati se necessario. Le funzioni a cui un utente ha accesso sono specificate dai ruoli. I ruoli preimpostati 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 Gestione utenti sono di sola lettura.

Tabella 4-4: Ruoli preimpostati

Ruolo	Attività tipiche
Amministratore	• Gestisce il sistema • Configura la sicurezza
Sviluppatore di metodi	• Crea i metodi • Esegue i lotti • Analizza i dati che devono essere utilizzati dall'utente
Analyst	• Esegue i lotti • Analizza i dati che devono essere utilizzati dall'utente
Revisore	• Controlla i dati • Controlla gli audit trail • Controlla i risultati della quantificazione

Tabella 4-5: Autorizzazioni preimpostate

Autorizzazione	Amministratore	Sviluppatore di metodi	Analyst	Revisore
Lotto				
Invia metodi sbloccati	✓	✓	✓	×
Apri	✓	✓	✓	✓
Salva con nome	✓	✓	✓	×
Invia	✓	✓	✓	×
Salva	✓	✓	✓	×
Salva tabella di riferimento ionica	✓	✓	✓	×
Aggiungi sottocartelle dati	✓	✓	✓	×
Configura regole di decisione	✓	✓	✓	×
Configurazione				
Scheda Generale	✓	✓	×	×
Generale: modifica impostazione regionale	✓	✓	×	×
Generale: modalità schermo intero	✓	✓	×	×
Generale: arresta i servizi Windows	✓	×	×	×
Scheda Comunicazione LIMS	✓	✓	×	×
Scheda mappe di audit	✓	×	×	×
Scheda Coda	✓	✓	✓	✓
Coda: tempo inattività strumento	✓	✓	×	×
Coda: numero max. di campioni acquisiti	✓	✓	×	×
Coda: altre impostazioni coda	✓	✓	×	×

Tabella 4-5: Autorizzazioni preimpostate (continua)

Autorizzazione	Amministratore	Sviluppatore di metodi	Analyst	Revisore
Scheda Progetti	✓	✓	✓	✓
Progetti: crea progetto	✓	✓	✓	×
Progetti: applica un modello mappa di audit a un progetto esistente	✓	×	×	×
Progetti: crea directory radice	✓	×	×	×
Progetti: imposta directory radice corrente	✓	×	×	×
Progetti: specifica credenziali di rete	✓	×	×	×
Progetti: abilita scrittura checksum per creazione dati wiff	✓	×	×	×
Progetti: cancella directory radice	✓	×	×	×
Scheda Dispositivi	✓	✓	✓	×
Scheda Gestione utenti	✓	×	×	×
Forza disconnessione utente	✓	×	×	×
Scheda CAC[1]	✓	×	×	×
Scheda Modelli di stampa	✓	✓	×	×
Modelli di stampa: crea e modifica modelli di stampa	✓	✓	×	×

[1] Nella versione 3.1, l'autorizzazione **Abilita amministrazione centrale** è stata rinominata in **CAC**. La pagina CAC nell'area di lavoro Configurazione consente di configurare l'amministrazione centrale del software SCIEX OS.

Tabella 4-5: Autorizzazioni preimpostate (continua)

Autorizzazione	Amministratore	Sviluppatore di metodi	Analyst	Revisore
Modelli di stampa: imposta modello di stampa predefinito	✓	✓	×	×
Modelli di stampa: applica il modello corrente a tutti i progetti nella directory radice	✓	×	×	×
Log eventi				
Accedi all'area di lavoro log eventi	✓	✓	✓	✓
Archivia log	✓	✓	✓	✓
Audit trail				
Accedi all'area di lavoro audit trail	✓	✓	✓	✓
Visualizza mappa di audit attiva	✓	✓	✓	✓
Stampa/Esporta audit trail	✓	✓	✓	✓
Pannello di acquisizione dati				
Inizio	✓	✓	✓	×
Interrompi	✓	✓	✓	×
Salva	✓	✓	✓	×
Metodo MS e LC				
Accedi all'area di lavoro metodo	✓	✓	✓	✓
Nuovo	✓	✓	×	×
Apri	✓	✓	✓	✓
Salva	✓	✓	×	×
Salva con nome	✓	✓	×	×
Blocca/Sblocca metodo	✓	✓	×	×
Coda				

Tabella 4-5: Autorizzazioni preimpostate (continua)

Autorizzazione	Amministratore	Sviluppatore di metodi	Analyst	Revisore
Gestisci	✓	✓	✓	×
Avvia/Arresta	✓	✓	✓	×
Stampa	✓	✓	✓	✓
Modifica campione	✓	✓	×	×
Libreria				
Accedi all'area di lavoro libreria	✓	✓	✓	✓
MS Tune				
Accedi all'area di lavoro MS Tune	✓	✓	✓	×
Tuning MS avanzato	✓	✓	×	×
Risoluzione dei problemi avanzata	✓	✓	×	×
Controllo stato rapido	✓	✓	✓	×
Ripristina dati strumento	✓	✓	×	×
Explorer				
Accedi all'area di lavoro Explorer	✓	✓	✓	✓
Esporta	✓	✓	✓	×
Stampa	✓	✓	✓	×
Opzioni	✓	✓	✓	×
Ricalibra	✓	✓	×	×
Analisi				
Nuovi risultati	✓	✓	✓	×
Crea metodo di elaborazione	✓	✓	✓	×
Modifica metodo di elaborazione	✓	✓	×	×

Tabella 4-5: Autorizzazioni preimpostate (continua)

Autorizzazione	Amministratore	Sviluppatore di metodi	Analyst	Revisore
Consenti l'esportazione e la creazione del report della tabella dei risultati sbloccata	✓	×	×	×
Salva risultati per lotto automazione	✓	✓	✓	×
Modifica algoritmo di integrazione metodo di quantificazione predefinito	✓	✓	×	×
Modifica parametri di integrazione metodo di quantificazione predefinito	✓	✓	×	×
Abilita avviso picco modificato progetto	✓	×	×	×
Aggiungi campioni	✓	✓	✓	×
Rimuovi campioni selezionati	✓	✓	✓	×
Esporta, importa o rimuovi calibrazione esterna	✓	✓	✓	×
Modifica nome campione	✓	✓	✓	×
Modifica tipo di campione	✓	✓	✓	×
Modifica ID campione	✓	✓	✓	×
Modifica concentrazione effettiva	✓	✓	✓	×
Modifica fattore di diluizione	✓	✓	✓	×
Modifica campi commento	✓	✓	✓	×
Abilita integrazione manuale	✓	✓	✓	×

Tabella 4-5: Autorizzazioni preimpostate (continua)

Autorizzazione	Amministratore	Sviluppatore di metodi	Analyst	Revisore
Imposta picco su non trovato	✓	✓	✓	×
Includi o escludi un picco dalla tabella dei risultati	✓	✓	✓	×
Opzioni di regressione	✓	✓	✓	×
Modifica parametri di integrazione tabella dei risultati per un singolo cromatogramma	✓	✓	✓	×
Modifica metodo di quantificazione per componente tabella dei risultati	✓	✓	✓	×
Crea nuove impostazioni tracciato metrico	✓	✓	✓	✓
Aggiungi colonne personalizzate	✓	✓	✓	×
Imposta formato titolo verifica picco	✓	×	×	×
Rimuovi colonna personalizzata	✓	✓	×	×
Impostazioni di visualizzazione tabella dei risultati	✓	✓	✓	✓
Blocca tabella dei risultati	✓	✓	✓	✓
Sblocca tabella dei risultati	✓	×	×	×
Contrassegna file dei risultati come rivisto e salva	✓	×	×	✓
Modifica modello report	✓	✓	×	×

Tabella 4-5: Autorizzazioni preimpostate (continua)

Autorizzazione	Amministratore	Sviluppatore di metodi	Analyst	Revisore
Trasferisci risultati a LIMS	✓	✓	✓	×
Modifica colonna codice a barre	✓	✓	×	×
Modifica assegnazione campione di confronto	✓	✓	×	×
Aggiungi gli spettri MSMS alla libreria	✓	✓	×	×
Impostazioni predefinite progetto	✓	✓	×	×
Crea report in tutti i formati	✓	✓	✓	✓
Modifica parametri criteri di segnalazione	✓	✓	✓	×
Modifica parametro di rimozione automatica anomalie	✓	✓	×	×
Abilita rimozione automatica anomalie	✓	✓	✓	×
Aggiorna metodo di trattamento tramite FF/LS	✓	✓	×	×
Aggiorna risultati tramite FF/LS	✓	✓	×	×
Abilita funzionalità di raggruppamento per addotti	✓	✓	×	×
Cerca file	✓	✓	✓	✓
Abilita aggiunta standard	✓	✓	✓	×
Imposta regola percentuale di integrazione manuale	✓	×	×	×

Tabella 4-5: Autorizzazioni preimpostate (continua)

Autorizzazione	Amministratore	Sviluppatore di metodi	Analyst	Revisore
Modifica peso/ volume	✓	✓	✓	×

Gestione utenti

Aggiunta di un utente o un gruppo

1. Aprire l'area di lavoro Configurazione.
2. Aprire la pagina Gestione utenti.
3. Aprire la scheda Utenti.
4. Fare clic su **Aggiungi utente** ( ).
   Viene visualizzata la finestra di dialogo Seleziona utente o gruppo.
5. Digitare il nome di un utente o di un gruppo, quindi fare clic su **OK**.

   Suggerimento! Per informazioni sulla finestra di dialogo Seleziona utente o gruppo e su come utilizzarla, premere **F1**.
6. Per rendere attivo un utente, accertarsi che la casella di controllo **Utente o gruppo attivo** sia selezionata.
7. Nell'area di lavoro **Ruoli**, selezionare un o più ruoli, quindi fare clic su **Salva**.

Disattivazione di utenti o gruppi

1. Aprire l'area di lavoro Configurazione.
2. Aprire la pagina Gestione utenti.
3. Aprire la scheda Utenti.
4. Nell'elenco **Nome utente o gruppo**, selezionare l'utente o il gruppo da disattivare.
5. Deselezionare la casella di controllo **Utente o gruppo attivo**.
   Il software chiede conferma.
6. Fare clic su **Sì**.

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, è necessario rimuoverlo anche dal software SCIEX OS.

1. Aprire l'area di lavoro Configurazione.
2. Aprire la pagina Gestione utenti.

3. Aprire la scheda Utenti.
4. Nell'elenco **Nome utente o gruppo** selezionare l'utente o il gruppo da rimuovere.
5. Fare clic su **Elimina**.
   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 Configurazione.
2. Aprire la pagina Gestione utenti.
3. Aprire la scheda Utenti.
4. Nel campo **Nome utente o gruppo** 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 **Salva**.

Creazione di un ruolo personalizzato

1. Aprire l'area di lavoro Configurazione.
2. Aprire la pagina Gestione utenti.
3. Aprire la scheda Ruoli.
4. Fare clic su **Aggiungi ruolo** ().
   Viene visualizzata la finestra di dialogo Duplica un ruolo utente.
5. Nel campo **Ruolo utente esistente**, 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 **Salva tutti i ruoli**.
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 Configurazione.

2. Aprire la pagina Gestione utenti.
3. Aprire la scheda Ruoli.
4. Fare clic su **Elimina un ruolo**.
   Viene visualizzata la finestra di dialogo Elimina un ruolo utente.
5. Selezionare il ruolo da eliminare e fare clic su **OK**.

Esportazione e importazione di impostazioni di gestione utenti

È possibile importare ed esportare il database User Management per il software SCIEX OS. 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 Configurazione.
2. Aprire la pagina Gestione utenti.
3. Fare clic su **Avanzate** > **Esporta impostazioni di gestione utenti**.
   Viene visualizzata la finestra di dialogo Esporta impostazioni di gestione utenti.
4. Fare clic su **Sfoglia**.
5. Cercare e selezionare la cartella in cui verranno salvate le impostazioni, quindi fare clic su **Seleziona cartella**.
6. Fare clic su **Esporta**.
   Viene mostrato un messaggio di conferma, con il nome del file che contiene le impostazioni esportate.
7. Fare clic su **OK**.

Importazione di impostazioni di gestione utenti

1. Aprire l'area di lavoro Configurazione.
2. Aprire la pagina Gestione utenti.
3. Fare clic su **Avanzate** > **Importa impostazioni di gestione utenti**.
   Viene visualizzata la finestra di dialogo Importa impostazioni di gestione utenti.
4. Fare clic su **Sfoglia**.
5. Cercare e selezionare il file che contiene le impostazioni da importare, quindi fare clic su **Apri**.
   Il software verifica che il file sia valido.

6. Fare clic su **Importa**.
   Il software esegue il backup delle impostazioni di gestione utenti correnti e importa le nuove impostazioni. Viene visualizzato un messaggio di conferma.
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 Configurazione.
2. Aprire la pagina Gestione utenti.
3. Fare clic su **Avanzate** > **Ripristina impostazioni precedenti**.
   Viene visualizzata la finestra di dialogo Ripristina impostazioni di gestione utenti.
4. Fare clic su **Sì**.
5. Chiudere e riaprire il software 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.

Tabella 4-6: Cartelle del progetto (continua)

Cartella	Contenuto
\Project Information	Contiene i file delle impostazioni predefinite del progetto.
\Quantitation Methods	Contiene tutti i file dei metodi di trattamento. I metodi di trattamento hanno l'estensione qmethod
\Quantitation Results	Contiene tutti i file della Tabella dei risultati di quantificazione. I file della Tabella dei risultati presentano l'estensione qsession.

Tipi di file del software

Per i tipi di file comuni nel software SCIEX OS, fare riferimento alla tabella: Tabella 4-7.

Tabella 4-7: File di SCIEX OS

Estensione	Tipo di file	Cartella
atds	• 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	• Per i progetti: *<project name>*\Audit Data • Per la workstation: C:\ProgramData\SCIEX\Audit Data
atms	Mappe di audit	• Per i progetti: *<project name>*\Audit Data • Per la workstation: C:\ProgramData\SCIEX\Audit Data
bch	Lotto	Batch
cset	Impostazioni Tabella dei risultati	Project Information
dad	File di dati relativi alla spettrometria di massa	• Optimization • Data
exml	Impostazioni predefinite progetto	Project Information
journal	File temporanei creati dal software SCIEX OS	Varie cartelle
lcm	Metodo LC	Acquisition Methods

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

Estensione	Tipo di file	Cartella
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 trattamento	Quantitation Methods
qsession	Tabella dei risultati **Nota:** Il software SCIEX OS può aprire solo i file qsession creati con il software SCIEX OS.	Quantitation Results
wiff	File di dati di spettrometria di massa compatibili con il software SCIEX OS **Nota:** Il software SCIEX OS crea sia file wiff che file wiff2.	Data
wiff.scan	File di dati relativi alla spettrometria di massa	• Optimization • Data
wiff2	File di dati relativi alla spettrometria di massa generati dal software SCIEX OS	• Optimization • Data
xls o xlsx	Foglio Excel	Batch
xps	Ricalibrazione	Data\Cal

Central Administrator Console 5

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. Non è tuttavia possibile installare il software CAC e il software SCIEX OS nella stessa workstation.

Utenti

Utilizzare la pagina Gestione utenti per aggiungere utenti e gruppi di Windows al database User Management per il software 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 accedere alla workstation e ottenere accesso al software SCIEX OS quando il software SCIEX OS è gestito dal 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 Amministrazione centrale.
2. Aprire la pagina Gestione utenti.
3. Aprire la scheda Pool utenti.
4. Fare clic su **Aggiungi utenti al pool utenti** ( ).
   Viene visualizzata la finestra di dialogo Seleziona utenti o gruppi.
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 Amministrazione centrale.
2. Aprire la pagina Gestione utenti.
3. Aprire la scheda Pool utenti.
4. Nel riquadro destro, selezionare l'utente o il gruppo da eliminare, quindi fare clic su **Elimina**.
   Il software chiede conferma.
5. Fare clic su **OK**.

Ruoli utente e autorizzazioni

Questa sezione descrive la pagina Ruoli utente e autorizzazioni.

Gli utenti possono essere assegnati a uno o più ruoli predefiniti, descritti nella tabella seguente, o se necessario, a ruoli personalizzati. Le funzioni a cui l'utente ha accesso sono specificate dai ruoli. I ruoli predefiniti non possono essere eliminati e le relative autorizzazioni non possono essere modificate.

Nota: Nel software Central Administrator Console (CAC), gli utenti possono anche visualizzare la versione precedente di SCIEX OS che supporta l'autorizzazione.

Tabella 5-1: Ruoli predefiniti

Ruolo	Attività tipiche
Amministratore	• Gestisce il sistema • Configura la sicurezza
Sviluppatore di metodi	• Crea i metodi • Esegue i lotti • Analizza i dati che devono essere utilizzati dall'utente
Installazione di **Analyst**	• Esegue i lotti • Analizza i dati che devono essere utilizzati dall'utente
Revisore	• Controlla i dati • Controlla gli audit trail • Controlla i risultati della quantificazione

Tabella 5-2: Autorizzazioni preimpostate

Autorizzazione	Amministratore	Sviluppatore di metodi	Installazione di Analyst	Revisore
Lotto				
Invia metodi sbloccati	✓	✓	✓	×
Apri	✓	✓	✓	✓
Salva con nome	✓	✓	✓	×
Invia	✓	✓	✓	×
Salva	✓	✓	✓	×
Salva tabella di riferimento ionica	✓	✓	✓	×
Aggiungi sottocartelle dati	✓	✓	✓	×
Configura regole di decisione	✓	✓	✓	×
Configurazione				
Scheda Generale	✓	✓	×	×
Generale: modifica impostazione regionale	✓	✓	×	×
Generale: modalità schermo intero	✓	✓	×	×
Scheda Comunicazione LIMS	✓	✓	×	×
Generale: arresta i servizi Windows	✓	×	×	×
Scheda mappe di audit	✓	×	×	×
Scheda Coda	✓	✓	✓	✓
Coda: tempo inattività strumento	✓	✓	×	×
Coda: numero max. di campioni acquisiti	✓	✓	×	×
Coda: altre impostazioni coda	✓	✓	×	×
Scheda Progetti	✓	✓	✓	✓

Tabella 5-2: Autorizzazioni preimpostate (continua)

Autorizzazione	Amministratore	Sviluppatore di metodi	Installazione di Analyst	Revisore
Progetti: crea progetto	✓	✓	✓	×
Progetti: applica un modello mappa di audit a un progetto esistente	✓	×	×	×
Progetti: crea directory radice	✓	×	×	×
Progetti: imposta directory radice corrente	✓	×	×	×
Progetti: specifica credenziali di rete	✓	×	×	×
Progetti: abilita scrittura checksum per creazione dati wiff	✓	×	×	×
Progetti: cancella directory radice	✓	×	×	×
Scheda Dispositivi	✓	✓	✓	×
Scheda Gestione utenti	✓	×	×	×
Forza disconnessione utente	✓	×	×	×
Scheda CAC[1]	✓	×	×	×
Scheda Modelli di stampa	✓	✓	×	×
Modelli di stampa: crea e modifica modelli di stampa	✓	✓	×	×
Modelli di stampa: imposta modello di stampa predefinito	✓	✓	×	×

[1] Nella versione 3.1, l'autorizzazione **Abilita amministrazione centrale** è stata rinominata in **CAC**. La pagina CAC nell'area di lavoro Configurazione consente di configurare l'amministrazione centrale del software SCIEX OS.

Tabella 5-2: Autorizzazioni preimpostate (continua)

Autorizzazione	Amministratore	Sviluppatore di metodi	Installazione di Analyst	Revisore
Modelli di stampa: applica il modello corrente a tutti i progetti nella directory radice	✓	×	×	×
Log eventi				
Accedi all'area di lavoro log eventi	✓	✓	✓	✓
Archivia log	✓	✓	✓	✓
Audit trail				
Accedi all'area di lavoro audit trail	✓	✓	✓	✓
Visualizza mappa di audit attiva	✓	✓	✓	✓
Stampa/Esporta audit trail	✓	✓	✓	✓
Pannello di acquisizione dati				
Inizio	✓	✓	✓	×
Interrompi	✓	✓	✓	×
Salva	✓	✓	✓	×
Metodo MS e LC				
Accedi all'area di lavoro metodo	✓	✓	✓	✓
Nuovo	✓	✓	×	×
Apri	✓	✓	✓	✓
Salva	✓	✓	×	×
Salva con nome	✓	✓	×	×
Blocca/Sblocca metodo	✓	✓	×	×
Coda				
Gestisci	✓	✓	✓	×
Avvia/Arresta	✓	✓	✓	×

Tabella 5-2: Autorizzazioni preimpostate (continua)

Autorizzazione	Amministratore	Sviluppatore di metodi	Installazione di Analyst	Revisore
Stampa	✓	✓	✓	✓
Modifica campione	✓	✓	×	×
Libreria				
Accedi all'area di lavoro libreria	✓	✓	✓	✓
MS Tune				
Accedi all'area di lavoro MS Tune	✓	✓	✓	×
Tuning MS avanzato	✓	✓	×	×
Risoluzione dei problemi avanzata	✓	✓	×	×
Controllo stato rapido	✓	✓	✓	×
Ripristina dati strumento	✓	✓	×	×
Analisi				
Nuovi risultati	✓	✓	✓	×
Crea metodo di elaborazione	✓	✓	✓	×
Modifica metodo di elaborazione	✓	✓	×	×
Consenti l'esportazione e la creazione del report della tabella dei risultati sbloccata	✓	×	×	×
Salva risultati per lotto automazione	✓	✓	✓	×
Modifica algoritmo di integrazione metodo di quantificazione predefinito	✓	✓	×	×
Modifica parametri di integrazione metodo di quantificazione predefinito	✓	✓	×	×

Tabella 5-2: Autorizzazioni preimpostate (continua)

Autorizzazione	Amministratore	Sviluppatore di metodi	Installazione di Analyst	Revisore
Abilita avviso picco modificato progetto	✓	×	×	×
Aggiungi campioni	✓	✓	✓	×
Rimuovi campioni selezionati	✓	✓	✓	×
Esporta, importa o rimuovi calibrazione esterna	✓	✓	✓	×
Modifica nome campione	✓	✓	✓	×
Modifica tipo di campione	✓	✓	✓	×
Modifica ID campione	✓	✓	✓	×
Modifica concentrazione effettiva	✓	✓	✓	×
Modifica fattore di diluizione	✓	✓	✓	×
Modifica campi commento	✓	✓	✓	×
Abilita integrazione manuale	✓	✓	✓	×
Imposta picco su non trovato	✓	✓	✓	×
Includi o escludi un picco dalla tabella dei risultati	✓	✓	✓	×
Opzioni di regressione	✓	✓	✓	×
Modifica parametri di integrazione tabella dei risultati per un singolo cromatogramma	✓	✓	✓	×

Tabella 5-2: Autorizzazioni preimpostate (continua)

Autorizzazione	Amministratore	Sviluppatore di metodi	Installazione di Analyst	Revisore
Modifica metodo di quantificazione per componente tabella dei risultati	✓	✓	✓	×
Crea nuove impostazioni tracciato metrico	✓	✓	✓	✓
Aggiungi colonne personalizzate	✓	✓	✓	×
Imposta formato titolo verifica picco	✓	×	×	×
Rimuovi colonna personalizzata	✓	✓	×	×
Impostazioni di visualizzazione tabella dei risultati	✓	✓	✓	✓
Blocca tabella dei risultati	✓	✓	✓	✓
Sblocca tabella dei risultati	✓	×	×	×
Contrassegna file dei risultati come rivisto e salva	✓	×	×	✓
Modifica modello report	✓	✓	×	×
Trasferisci risultati a LIMS	✓	✓	✓	×
Modifica colonna codice a barre	✓	✓	×	×
Modifica assegnazione campione di confronto	✓	✓	×	×
Aggiungi gli spettri MSMS alla libreria	✓	✓	×	×
Impostazioni predefinite progetto	✓	✓	×	×

Tabella 5-2: Autorizzazioni preimpostate (continua)

Autorizzazione	Amministratore	Sviluppatore di metodi	Installazione di Analyst	Revisore
Crea report in tutti i formati	✓	✓	✓	✓
Modifica parametri criteri di segnalazione	✓	✓	✓	×
Modifica parametro di rimozione automatica anomalie	✓	✓	×	×
Abilita rimozione automatica anomalie	✓	✓	✓	×
Aggiorna metodo di trattamento tramite FF/LS	✓	✓	×	×
Aggiorna risultati tramite FF/LS	✓	✓	×	×
Abilita funzionalità di raggruppamento per addotti	✓	✓	×	×
Cerca file	✓	✓	✓	✓
Abilita aggiunta standard	✓	✓	✓	×
Imposta regola percentuale di integrazione manuale	✓	×	×	×
Modifica peso/volume	✓	✓	✓	×
Explorer				
Accedi all'area di lavoro Explorer	✓	✓	✓	✓
Esporta	✓	✓	✓	×
Stampa	✓	✓	✓	×
Opzioni	✓	✓	✓	×
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 Amministrazione centrale.
2. Aprire la pagina Gestione utenti.
3. Aprire la scheda Ruoli utente e autorizzazioni.
4. Fare clic su **Aggiungi ruolo** ().
   Viene visualizzata la finestra di dialogo Duplica un ruolo utente.
5. Nel campo **Ruolo utente esistente**, 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 Ruoli utente e categorie di autorizzazione.
7. Selezionare i privilegi di accesso per il ruolo selezionando le caselle di controllo appropriate.
8. Fare clic su **Salva tutti i ruoli**.

Eliminazione di un ruolo personalizzato

1. Aprire l'area di lavoro Amministrazione centrale.
2. Aprire la pagina Gestione utenti.
3. Aprire la scheda Ruoli utente e autorizzazioni.
4. Fare clic su **Elimina un ruolo**.
   Viene visualizzata la finestra di dialogo Elimina un ruolo utente.
5. Selezionare il ruolo da eliminare e fare clic su **OK**.

Gruppi di lavoro

Utilizzare la pagina Gestione gruppi di lavoro 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 il software SCIEX OS.

Creazione di un gruppo di lavoro

1. Aprire l'area di lavoro Amministrazione centrale.
2. Aprire la pagina Gestione gruppi di lavoro.
3. Fare clic su **Aggiungi gruppo di lavoro** ().
   Viene visualizzata la finestra di dialogo Aggiungi un gruppo di lavoro.
4. Inserire un nome nel campo **Nome gruppo di lavoro**.
5. Digitare una descrizione nel campo **Descrizione**, quindi fare clic su **Aggiungi**.
   Il gruppo di lavoro viene creato e aggiunto al riquadro Gestisci gruppi di lavoro e assegnazioni. Il software Central Administrator Console (CAC) crea il nome del gruppo di lavoro appropriato sul server.

   Nota: La modalità integrata 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 Amministrazione centrale.
2. Aprire la pagina Gestione gruppi di lavoro.
3. Espandere l'elenco **Gruppi di lavoro** e trovare il gruppo di lavoro da eliminare. Fare clic su **Elimina**.
   Viene visualizzata la finestra di dialogo Elimina gruppo di lavoro.
4. Fare clic su **Sì**.

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 Amministrazione centrale.
2. Aprire la pagina Gestione gruppi di lavoro.

3. Nel riquadro Gestisci gruppi di lavoro e assegnazioni, espandere il gruppo di lavoro da modificare, quindi espandere l'elenco **Utenti**.
4. Selezionare un utente o un gruppo, quindi fare clic su **Aggiungi** (>).

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

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

Aggiunta o rimozione di un ruolo

Procedure preliminari
• 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 Amministrazione centrale.
2. Aprire la pagina Gestione gruppi di lavoro.
3. Nel riquadro Gestisci gruppi di lavoro e assegnazioni, espandere il gruppo di lavoro da modificare, quindi espandere l'elenco **Utenti**.
4. Nella sezione Appartenenza gruppo di lavoro corrente, assegnare o rimuovere ruoli nella colonna **Assegna ruoli**.
5. Fare clic su **Salva**.

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 Amministrazione centrale.
2. Aprire la pagina Gestione gruppi di lavoro.
3. Nel riquadro Gestisci gruppi di lavoro e assegnazioni, espandere il gruppo di lavoro da modificare, quindi espandere l'elenco **Workstation**.
4. Selezionare una workstation, quindi fare clic su **Aggiungi** (>).
   La workstation viene aggiunta al gruppo di lavoro corrente.

5. Fare clic su **Salva**.

Assegnazione di impostazioni di sicurezza gruppo di lavoro

Procedure preliminari
• 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 Amministrazione centrale.
2. Aprire la pagina Gestione gruppi di lavoro.
3. Nel riquadro Gestisci gruppi di lavoro e assegnazioni, espandere il gruppo di lavoro da modificare, quindi espandere l'elenco **Workstation**.
4. (Facoltativo) Per impostare come predefinito il gruppo di lavoro corrente per quella workstation, selezionare la casella di controllo **Imposta come predefinito** nella sezione Appartenenza gruppo di lavoro corrente.
5. Nella sezione Assegna impostazioni di sicurezza, selezionare la **Modalità sicurezza** per il gruppo di lavoro, quindi digitare l'ora appropriata per **Blocco schermo** e **Disconnessione automatica**.
6. Fare clic su **Salva**.

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 Amministrazione centrale.
2. Aprire la pagina Gestione gruppi di lavoro.
3. Nel riquadro Gestisci gruppi di lavoro e assegnazioni, espandere il gruppo di lavoro da modificare, quindi espandere l'elenco **Progetti**.
4. Selezionare la casella di controllo **Utilizza impostazioni centrali per i progetti**. Viene mostrata la sezione di selezione del progetto.
5. Selezionare una **Directory radice progetto** 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 **Aggiungi** () per aggiungere i progetti al gruppo di lavoro.
   La cartella radice del progetto viene aggiunta alla tabella Appartenenza gruppo di lavoro corrente. Espandere la radice del progetto per mostrare i progetti correnti nel gruppo di lavoro.
7. Fare clic su **Salva**.

Gestione dei progetti

Utilizzare la pagina Gestione progetto 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 Pool radice progetto 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 Pool radice progetto 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 Amministrazione centrale.
2. Aprire la pagina Gestione progetto.
3. Fare clic su **Aggiungi radice progetto nuova o esistente al pool progetti** ().
   Viene visualizzata la finestra di dialogo Aggiungi directory radice.
4. Digitare il percorso completo della directory radice, quindi fare clic su **OK**.

La cartella è stata creata.

Suggerimento! Anziché digitare il percorso, fare clic su **Sfoglia** 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 del software 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 Amministrazione centrale.
2. Aprire la pagina Gestione progetto.
3. Trovare la directory radice del progetto da eliminare, quindi fare clic su **Elimina radice progetto** nella sezione Azioni.
   Il software chiede conferma.
4. Fare clic su **OK**.

Aggiunta di un progetto

Procedure preliminari
• Aggiunta di una directory radice

Il progetto memorizza metodi di acquisizione, dati, lotti, metodi di trattamento, risultati del trattamento 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 Amministrazione centrale.
2. Aprire la pagina Gestione progetto.
3. Fare clic su **Aggiungi progetto** nella sezione Azioni della cartella radice.
   Viene visualizzata la finestra di dialogo Nuovo progetto.

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 Amministrazione centrale.
2. Aprire la pagina Gestione progetto.
3. Fare clic su **Aggiungi sottocartelle dati** nella sezione Azioni della cartella radice.
   Viene visualizzata la finestra di dialogo Aggiungi sottocartelle dati.
4. Selezionare un progetto a cui apparterrà la sottocartella.
5. Fare clic su **Aggiungi una nuova sottocartella dati** ().
   Viene visualizzata la finestra di dialogo Nome sottocartella dati.
6. Digitare il nome della sottocartella
7. Fare clic su **Salva**.

   Suggerimento! Le sottocartelle possono essere annidate all'interno di altre sottocartelle. Per creare una sottocartella annidata, selezionare una sottocartella esistente nella sezione Sottocartelle dati progetto, quindi fare clic su **Aggiungi una nuova sottocartella dati** ().

8. Chiudere la finestra di dialogo Aggiungi sottocartelle dati.

Workstation

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

Aggiunta di una workstation

Nella pagina Gestione workstation gli amministratori possono aggiungere workstation, abilitare e disabilitare il controllo centrale delle workstation e rimuovere workstation.

1. Aprire l'area di lavoro Amministrazione centrale.
2. Aprire la pagina Gestione workstation.
3. Fare clic su **Aggiungi workstation al pool workstation** ().
   Viene visualizzata la finestra di dialogo Seleziona computer.
4. Digitare i nomi delle workstation da aggiungere, quindi fare clic su **OK**.

L'amministrazione centrale **Stato** della workstation passa da **Connessione in corso** a **Disabilitato**.

5. (Opzionale) Per abilitare il controllo centrale della workstation:
   a. Nella colonna **Stato** fare clic su **Disabilitato**.
   b. Fare clic su **OK**.

Suggerimento! Gli utenti possono anche abilitare l'amministrazione centrale nel software SCIEX OS. Fare riferimento al documento: *Guida online del software SCIEX OS*.

Eliminazione di una workstation

Se una workstation non è più in uso o non è più richiesta come parte di un gruppo di lavoro, eliminarla dal relativo pool workstation. Se si elimina una workstation, questa viene rimossa da ogni gruppo di lavoro a cui era assegnata. Alla rimozione della workstation, nessuno dei dati in essa memorizzati andrà perduto.

1. Aprire l'area di lavoro Amministrazione centrale.
2. Aprire la pagina Gestione workstation.
3. Fare clic su **Gestione workstation**.
4. Nel riquadro Pool workstation trovare la workstation da eliminare, quindi fare clic su **Elimina**.
   Viene visualizzata la finestra di dialogo Elimina workstation.
5. Fare clic su **OK**.

Report e funzionalità di sicurezza

Generazione di report di dati

Utilizzare questa procedura per generare report di dati contenenti dettagli quali utenti configurati, ruoli, workstation, progetti e gruppi di lavoro.

1. Aprire l'area di lavoro Amministrazione centrale.
2. Fare clic su **Stampa**.
   Viene visualizzata la finestra di dialogo Opzioni di stampa.
3. Seleziona le pagine da stampare, quindi fare clic su **Continua**.
4. Impostare le opzioni di stampa, quindi fare clic su **Stampa**.
5. (Solo Stampa su PDF) Spostarsi sul percorso in cui il report verrà salvato, quindi fare clic su **Salva**.

Esportazione delle impostazioni software CAC

Utilizzare questa procedura per esportare le impostazioni di sicurezza in modo che possano essere importate in un altro sistema Central Administrator Console (CAC). Le impostazioni sono esportate come file `ecac`.

1. Aprire l'area di lavoro Amministrazione centrale.
2. Fare clic su **Avanzate** > **Esporta impostazioni CAC**.
   Viene visualizzata la finestra di dialogo Esporta impostazioni CAC.
3. Fare clic su **Sfoglia**.
4. Cercare e selezionare la cartella in cui verranno salvate le impostazioni, quindi fare clic su **Seleziona cartella**.
5. Fare clic su **Esporta**.
   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
• Esportazione delle impostazioni software CAC

Utilizzare questa procedura per importare le impostazioni di sicurezza da altri sistemi Central Administrator Console (CAC). Le impostazioni sono importate da un file `ecac`.

1. Aprire l'area di lavoro Amministrazione centrale.
2. Aprire l'area di lavoro Configurazione.
3. Aprire la pagina Gestione utenti.
4. Fare clic su **Avanzate** > **Importa impostazioni CAC**.
   Viene visualizzata la finestra di dialogo Importa impostazioni CAC.
5. Fare clic su **Sfoglia**.
6. Cercare e selezionare il file che contiene le impostazioni da importare, quindi fare clic su **Apri**.
   Il software verifica che il file sia valido.
7. Fare clic su **Importa**.
   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.
8. Fare clic su **OK**.

Ripristino delle impostazioni del software CAC

Utilizzare questa procedura per importare automaticamente le impostazioni `ecac` esportate per ultime.

1. Aprire l'area di lavoro Amministrazione centrale.
2. Fare clic su **Avanzate** > **Ripristina impostazioni CAC**.
   Viene visualizzata la finestra di dialogo Ripristina impostazioni CAC.

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

3. Fare clic su **Sì**.

Esportazione delle impostazioni di gestione utenti CAC

Utilizzare questa procedura per esportare le impostazioni di gestione utenti che potranno essere applicate a un altro sistema Central Administrator Console (CAC). Le impostazioni sono esportate come file `data`.

Nota: È possibile importare le impostazioni esportate in un sistema utilizzando la stessa versione del software CAC.

1. Aprire l'area di lavoro Gestione configurazione.
2. Fare clic su **Avanzate** > **Esporta impostazioni di gestione utenti**.
   Viene visualizzata la finestra di dialogo Esporta impostazioni CAC.
3. Fare clic su **Sfoglia**.
4. Cercare e selezionare la cartella in cui verranno salvate le impostazioni, quindi fare clic su **Seleziona cartella**.
5. Fare clic su **Esporta**.
   Viene mostrato un messaggio di conferma, con il nome del file che contiene le impostazioni esportate.
6. Fare clic su **OK**.

Importazione delle impostazioni di gestione utenti CAC

Procedure preliminari
• Esportazione delle impostazioni di gestione utenti CAC

Utilizzare questa procedura per importare le impostazioni di sicurezza da un altro sistema Central Administrator Console (CAC). Le impostazioni vengono importate da un file `data`.

Nota: È possibile importare le impostazioni esportate in un sistema utilizzando la stessa versione del software CAC.

1. Aprire l'area di lavoro Gestione configurazione.
2. Fare clic su **Avanzate** > **Importa impostazioni di gestione utenti**.
   Viene visualizzata la finestra di dialogo Importa impostazioni di gestione utenti.
3. Fare clic su **Sfoglia**.
4. Cercare e selezionare il file che contiene le impostazioni da importare, quindi fare clic su **Apri**.
   Il software verifica che il file sia valido.
5. Fare clic su **Importa**.
   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**.

Acquisizione di rete 6

In questa sezione vengono descritti il funzionamento dell'acquisizione di rete nel software SCIEX OS e i benefici e i limiti dei progetti basati sulla 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 trattare da workstation 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.

Tuttavia, in assenza di accesso con diritti di eliminazione a questa cartella, il software SCIEX OS non può funzionare in modo ottimale. 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 per il software SCIEX OS.

Lo SNA viene specificato nella pagina Progetti nell'area di lavoro Configurazione. È possibile specificare un solo account di dominio o di rete Windows.

Se non è specificato uno SNA, il software 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 viene 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 archivia i dati. Per garantire un'archiviazione sicura delle informazioni del progetto, creare la directory radice con il software SCIEX OS. Non creare progetti in File Explorer.

Facoltativamente, quando si creano directory radice su una risorsa di rete, definire **Credenziali per account di rete sicuro**. 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: *Guida per l'utente del software SCIEX OS*.

Specificare un account di rete sicuro

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 Configurazione.
2. Fare clic su **Progetti**.
3. Nella sezione **Avanzate**, fare clic su **Credenziali per account di rete sicuro**.
4. Digitare nome utente, password e dominio dell'account di rete sicuro definito nella risorsa di rete.
5. Fare clic su **OK**.

Auditing 7

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

Il software organizza gli eventi di audit nell'area di lavoro Audit trail. Il software archivia gli eventi in audit trail, ovvero file contenenti i record degli eventi sottoposti a audit.

Gli eventi di workstation sono memorizzati nell'audit trail workstation. Gli audit trail workstation sono file che archiviano gli eventi controllati per il computer in cui è installato il software SCIEX OS.

Gli eventi del sistema CAC sono archiviati nell'audit trail CAC.

Gli eventi di progetto sono memorizzati nell'audit trail di progetto. L'area di lavoro Audit trail mostra gli audit trail per i progetti nella directory radice attiva. Gli eventi di audit trail di elaborazione sono contenuti nell'audit trail di progetto e archiviati nella Tabella dei risultati.

Per un elenco completo degli eventi di audit, fare riferimento alla sezione: Eventi di audit.

Gli audit trail, associati a file quali i file `wiff2` e i file della Tabella dei risultati, 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)	• Modifiche di:
	  • Assegnazione mappa di audit attiva
	  • Tuning dello strumento
	  • Code dei campioni
	  • Sicurezza
	  • Tuning
	  • Dispositivi
		• Cartella `C:\ProgramData\SCIEX\Audit Data`	• Nessuna mappa di audit

Tabella 7-1: Audit Trail (continua)

Audit trail	Esempi di eventi registrati	Mappe di audit disponibili memorizzate in	Mappe di audit predefinite

CAC	• Modifiche di:
	  • Mappa di audit
	  • CAC
	  • Sicurezza
	  • Log utenti
		• Cartella `C:\ProgramData\SCIEX\Audit Data`	• Mappa di audit muta

Progetto (uno per progetto)	• Modifiche di:
	  • Assegnazione mappa di audit attiva (SCIEX OS)
	  • Progetto
	  • Dati
	• Stampa
		• Cartella `<project>\Audit Data`	• Specificato nella pagina Mappe di audit dell'area di lavoro Configurazione

Quando un audit trail contiene 20.000 record di audit, il software SCIEX OS e CAC archivia automaticamente i record e inizia 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. Nel software SCIEX OS sono disponibili due tipi di mappe di audit: workstation e progetto. Nel software CAC sono disponibili due tipi di mappe di audit: CAC 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, ma solo una mappa di audit può essere utilizzata in un determinato momento per ogni workstation, sistema CAC e ogni progetto. La mappa di audit in uso per una workstation, sistema CAC o progetto viene definita mappa di audit attiva.

Quando è installato il software SCIEX OS, la mappa di audit predefinita per tutti i progetti è Nessuna mappa di audit. Quando il software CAC è installato, la mappa di audit predefinita per tutti i nuovi progetti è Mappa di audit muta. 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 applicabili 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 siano disponibili una mappa di audit per la workstation o l'audit trail CAC e una per ogni progetto.

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

Attività	Fare riferimento a

• SCIEX OS: creare una mappa di audit per l'audi trail della workstation.
• Software CAC: creare una mappa di audit per l'audit trail CAC.
	• SCIEX OS:
	  • Creazione di una mappa di audit per la workstation
	  • Modifica di una mappa di audit della workstation
	• Software CAC:
	  • Creazione di una mappa di audit CAC
	  • Modifica di una mappa di audit CAC

• SCIEX OS: applicare la mappa di audit all'audit trail della workstation. • Software CAC: applicare la mappa di audit all'audit trail CAC.	• SCIEX OS: Modifica della mappa di audit attiva per una workstation • Software CAC: Modifica della mappa di audit attiva per un sistema CAC
Creare una mappa di audit attiva predefinita per nuovi progetti.	• Creazione di una mappa di audit di progetto.
Configurare la mappa di audit da utilizzare per ogni progetto esistente.	• 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.	• 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
Mappa di audit di esempio	Gli eventi selezionati vengono controllati. Esclusivamente a scopo illustrativo.
Mappa di audit completa	Tutti gli eventi vengono controllati. Tutti gli eventi richiedono firme elettroniche e ragioni.
Nessuna mappa di audit	Nessun evento viene controllato. **Nota:** L'evento **Modifica assegnazione mappa di audit attiva** viene sempre registrato, anche se non viene usato alcun modello di mappa di audit.
Mappa di audit muta	Tutti gli eventi vengono controllati. Per gli eventi non sono richieste né firme elettroniche né motivi.

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 SCIEX OS.

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: Audit trail del progetto.

Creazione di una mappa di audit di progetto

1. Aprire l'area di lavoro Configurazione.
2. Fare clic su **Mappe di audit**.
3. Aprire la scheda Modelli di progetti.

4. Nel campo **Modifica modello di mappa**, selezionare un modello da utilizzare come base per la nuova mappa.
5. Fare clic su **Aggiungi modello** ().
   Viene visualizzata la finestra di dialogo Aggiungi modello mappa di audit progetto.
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 **Sottoposto a audit** per l'evento.
   b. (Facoltativo) Se è richiesto un motivo, selezionare **Motivo richiesto**.
   c. (Facoltativo) Se è richiesta una firma elettronica, selezionare **Firma elettronica richiesta**.
   d. (Facoltativo) Se sono richiesti motivi predefiniti, selezionare **Utilizza solo il motivo predefinito** e definire i motivi.
8. Assicurarsi che la casella di controllo **Sottoposto a audit** sia vuota per gli eventi che non verranno controllati.
9. Fare clic su **Salva modello**.
   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 **Sì**, selezionare i progetti che utilizzeranno la nuova mappa, quindi fare clic su **Applica**.
    - Se la nuova mappa non deve essere applicata ai progetti esistenti, fare clic su **No**.
11. (Facoltativo) Per utilizzare questa mappa di audit come predefinita per tutti i nuovi progetti, fare clic su **Utilizza come valore predefinito per i nuovi progetti**.

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 Configurazione.
2. Fare clic su **Mappe di audit**.
3. Aprire la scheda Modelli di progetti.
4. Nel campo **Modifica modello di mappa**, selezionare la mappa da modificare.
5. Selezionare e configurare gli eventi da registrare effettuando le seguenti operazioni:
   a. Selezionare la casella di controllo **Sottoposto a audit** per l'evento.
   b. (Facoltativo) Se è richiesto un motivo, selezionare **Motivo richiesto**.
   c. (Facoltativo) Se è richiesta una firma elettronica, selezionare **Firma elettronica richiesta**.

d. (Facoltativo) Se sono richiesti motivi predefiniti, selezionare **Utilizza solo il motivo predefinito** e definire i motivi.

6. Assicurarsi che la casella di controllo **Sottoposto a audit** sia vuota per gli eventi che non verranno controllati.
7. Fare clic su **Salva modello**.
   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 **Sì**, selezionare i progetti che utilizzeranno la nuova mappa, quindi fare clic su **Applica**.
   - 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 Configurazione.
2. Fare clic su **Mappe di audit**.
3. Aprire la scheda Modelli di progetti.
4. Nel campo **Modifica modello di mappa**, selezionare la mappa di audit da assegnare al progetto.
5. Fare clic su **Applica ai progetti esistenti**.
   Viene visualizzata la finestra di dialogo Applica modello mappa di audit progetto.
6. Selezionare le caselle di controllo relative ai progetti che si riferiscono a questa mappa di audit.
7. Fare clic su **Applica**.

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 Configurazione.
2. Fare clic su **Mappe di audit**.
3. Aprire la scheda Modelli di progetti.
4. Nel campo **Modifica modello di mappa** selezionare la mappa da eliminare.
5. Fare clic su **Elimina modello**.
   Il sistema richiede conferma.
6. Fare clic su **Sì**.

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: Audit trail workstation.

Creazione di una mappa di audit per la workstation

1. Aprire l'area di lavoro Configurazione.
2. Fare clic su **Mappe di audit**.
3. Aprire la scheda Modelli di workstation.
4. Nel campo **Modifica modello di mappa**, selezionare un modello da utilizzare come base per la nuova mappa.
5. Fare clic su **Aggiungi modello** ().
   Viene visualizzata la finestra di dialogo Aggiungi un modello mappa di audit workstation.
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 **Sottoposto a audit** per l'evento.
   b. (Facoltativo) Se è richiesto un motivo, selezionare **Motivo richiesto**.
   c. (Facoltativo) Se è richiesta una firma elettronica, selezionare **Firma elettronica richiesta**.
   d. (Facoltativo) Se sono richiesti motivi predefiniti, selezionare **Utilizza solo il motivo predefinito** e definire i motivi.
8. Assicurarsi che la casella di controllo **Sottoposto a audit** sia vuota per gli eventi che non verranno controllati.
9. Fare clic su **Salva modello**.
10. (Facoltativo) Per rendere la presente mappa di audit attiva per la workstation, fare clic su **Applica alla 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 Configurazione.
2. Fare clic su **Mappe di audit**.
3. Aprire la scheda Modelli di workstation.
4. Nel campo **Modifica modello di mappa** selezionare la mappa da modificare.
5. Selezionare e configurare gli eventi da registrare effettuando le seguenti operazioni:
   a. Selezionare la casella di controllo **Sottoposto a audit** per l'evento.

b. (Facoltativo) Se è richiesto un motivo, selezionare **Motivo richiesto**.

c. (Facoltativo) Se è richiesta una firma elettronica, selezionare **Firma elettronica richiesta**.

d. (Facoltativo) Se sono richiesti motivi predefiniti, selezionare **Utilizza solo il motivo predefinito** e definire i motivi.

6. Assicurarsi che la casella di controllo **Sottoposto a audit** sia vuota per gli eventi che non verranno controllati.
7. Fare clic su **Salva modello**.
8. (Facoltativo) Per rendere la presente mappa di audit attiva per la workstation, fare clic su **Applica alla 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 Configurazione.
2. Fare clic su **Mappe di audit**.
3. Aprire la scheda Modelli di workstation.
4. Nel campo **Modifica modello di mappa**, selezionare la mappa da applicare alla workstation.
5. Fare clic su **Applica alla 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 Configurazione.
2. Fare clic su **Mappe di audit**.
3. Aprire la scheda Modelli di workstation.
4. Nel campo **Modifica modello di mappa** selezionare la mappa da eliminare.
5. Fare clic su **Elimina modello**.
   Il sistema richiede conferma.
6. Fare clic su **Sì**.

Mappe di audit CAC

Le mappe di audit CAC controllano l'auditing degli eventi della workstation CAC. Per un elenco degli eventi sottoponibili a auditing, fare riferimento alla sezione: Audit trail workstation.

Creazione di una mappa di audit CAC

1. Aprire l'area di lavoro Configurazione.
2. Fare clic su **Mappe di audit**.
3. Aprire la scheda Modelli CAC.
4. Nel campo **Modifica modello di mappa**, selezionare un modello da utilizzare come base per la nuova mappa.
5. Fare clic su **Aggiungi modello** ( ).
   Viene visualizzata la finestra di dialogo Aggiungi un modello mappa di audit CAC .
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 **Sottoposto a audit** per l'evento.
   b. (Facoltativo) Se è richiesto un motivo, selezionare **Motivo richiesto**.
   c. (Facoltativo) Se è richiesta una firma elettronica, selezionare **Firma elettronica richiesta**.
   d. (Facoltativo) Se sono richiesti motivi predefiniti, selezionare **Utilizza solo il motivo predefinito** e definire i motivi.
8. Assicurarsi che la casella di controllo **Sottoposto a audit** sia vuota per gli eventi che non verranno controllati.
9. Fare clic su **Salva modello**.
10. (Facoltativo) Per utilizzare la mappa di audit come mappa di audit attiva per la workstation CAC, fare clic su **Applica alla CAC** .

Modifica di una mappa di audit CAC

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

1. Aprire l'area di lavoro Configurazione.
2. Fare clic su **Mappe di audit**.
3. Aprire la scheda Modelli CAC.
4. Nel campo **Modifica modello di mappa** selezionare la mappa da modificare.
5. Selezionare e configurare gli eventi da registrare effettuando le seguenti operazioni:
   a. Selezionare la casella di controllo **Sottoposto a audit** per l'evento.
   b. (Facoltativo) Se è richiesto un motivo, selezionare **Motivo richiesto**.
   c. (Facoltativo) Se è richiesta una firma elettronica, selezionare **Firma elettronica richiesta**.

d. (Facoltativo) Se sono richiesti motivi predefiniti, selezionare **Utilizza solo il motivo predefinito** e definire i motivi.

6. Assicurarsi che la casella di controllo **Sottoposto a audit** sia vuota per gli eventi che non verranno controllati.
7. Fare clic su **Salva modello**.
8. (Facoltativo) Per utilizzare la mappa di audit come mappa di audit attiva per la workstation CAC, fare clic su **Applica alla CAC** .

Modifica della mappa di audit attiva per un sistema CAC

Quando si applica una mappa di audit alla workstation CAC, 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 Configurazione.
2. Fare clic su **Mappe di audit**.
3. Aprire la scheda Modelli CAC.
4. Nel campo **Modifica modello di mappa** selezionare la mappa da applicare alla workstation CAC.
5. Fare clic su **Applica alla CAC** .

Eliminazione di una mappa di audit CAC

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

1. Aprire l'area di lavoro Configurazione.
2. Fare clic su **Mappe di audit**.
3. Aprire la scheda Modelli CAC.
4. Nel campo **Modifica modello di mappa** selezionare la mappa da eliminare.
5. Fare clic su **Elimina modello**.
   Il sistema richiede conferma.
6. Fare clic su **Sì**.

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 dei record audit trail

1. Aprire l'area di lavoro Audit trail.

2. Nel riquadro di sinistra, fare clic sull'audit trail da visualizzare.
3. Per visualizzare informazioni dettagliate su un evento di audit, fare clic sull'evento.

   Il tipo di evento selezionato controlla le informazioni visualizzate. Le informazioni sono visualizzate in una o più delle schede seguenti.

Tabella 7-4: Schede dettagli eventi

Scheda	Informazioni
Dettagli generali	Mostra informazioni quali la differenza di fuso orario e il nome della workstation.
Prima della modifica	Mostra il contenuto prima della modifica.
Dopo la modifica	Mostra il contenuto dopo la modifica.
Dettagli modifiche	Mostra il contenuto originale e il nuovo contenuto nello stesso riquadro. In Visualizzazione differenza il contenuto originale è visualizzato in rosso e il contenuto nuovo in verde. In Visualizzazione affiancata il contenuto originale e nuovo sono visualizzati in riquadri separati, per consentire all'utente di vedere più agevolmente le modifiche.

Ricerca o filtro dei record di audit

1. Aprire l'area di lavoro Audit trail.
2. Selezionare l'audit trail da cercare.
3. Per cercare un record di audit specifico, digitare il testo nel campo **Trova nella pagina**. 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 Filtra 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 di audit, 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 file di un audit trail archiviato della workstation presenta il formato `WorkstationAuditTrailData-<workstation name>-<YYYY><MMDDHHMMSS>.atds`.

Questa procedura può essere utilizzata anche per aprire un audit trail per una Tabella dei risultati.

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

Nota: Per aprire un audit trail per una Tabella dei risultati, 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 **Stampa**.
   Viene visualizzata la finestra di dialogo Stampa.
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 **Esporta**.
4. Selezionare il percorso in cui il file esportato verrà archiviato, digitare un **Nome file** e fare clic su **Salva**.
   L'audit trail viene salvato come file .csv (valore separato da virgola).

Record degli audit trail SCIEX OS

Questa sezione descrive i campi dei record di audit trail.

Gli audit trail 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 7-5: Campi dei record di audit

Etichetta	Descrizione
Indicatore ora	Data e ora di creazione del record.
Nome evento	Il nome dell'evento.
Descrizione	Una descrizione dell'evento.
Motivo	Il motivo fornito per l'evento.
Firma elettronica	Se è stata inserita una firma elettronica per l'evento.

Tabella 7-5: Campi dei record di audit (continua)

Etichetta	Descrizione
Nome utente completo	Il nome dell'utente. **Nota:** Per gli eventi attivati da una regola di decisione, questo è l'utente che ha inviato il lotto.
Utente	L'ID dell'utente che ha avviato l'evento che ha generato il record.
Categoria	La funzione o la categoria a cui appartiene l'evento.

Il riquadro inferiore dell'area di lavoro Audit trail mostra informazioni dettagliate su un evento selezionato, inclusi dettagli di eventuali modifiche, se applicabile.

Per gli elenchi di tutti gli eventi registrati nella workstation e negli audit trail del progetto, fare riferimento alle sezioni: Audit trail workstation e Audit trail del progetto.

Record degli audit trail CAC

Questa sezione descrive i campi dei record di audit trail.

Gli audit trail CAC e del progetto sono file crittografati.

Nota: Gli archivi e gli audit trail CAC 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 7-6: Campi dei record di audit

Etichetta	Descrizione
Indicatore ora	Data e ora di creazione del record.
Nome evento	Il nome dell'evento.
Descrizione	Una descrizione dell'evento.
Motivo	Il motivo fornito per l'evento.
Firma elettronica	Se è stata inserita una firma elettronica per l'evento.
Nome utente completo	Il nome dell'utente. **Nota:** Per gli eventi attivati da una regola di decisione, questo è l'utente che ha inviato il lotto.
Utente	L'ID dell'utente che ha avviato l'evento che ha generato il record.
Categoria	La funzione o la categoria a cui appartiene l'evento.

Il riquadro inferiore dell'area di lavoro Audit trail mostra informazioni dettagliate su un evento selezionato, inclusi dettagli di eventuali modifiche, se applicabile.

Per elenchi di tutti gli eventi registrati negli audit trail CAC e di progetto, fare riferimento alle sezioni: Tabella 3 e Audit trail del progetto.

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 dell'audit trail della workstation sono contenuti nella cartella `C:\ProgramData\SCIEX\Audit Data`. I nomi file hanno il formato WorkstationAuditTrailData-<*nome workstation*>-<*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 e trattamento 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 trattati 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 per 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 Coda.
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. Aprire il software SCIEX OS.
   Entro 15 minuti, il software 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.

Autorizzazioni di Windows B

Questa sezione fornisce un elenco delle autorizzazioni di Windows richieste per ogni ruolo utente e per l'utente SYSTEM, per il corretto funzionamento del software SCIEX OS.

Nota: Il percorso predefinito della cartella *Installed Root Directory* è `D:\SCIEX OS Data`.

Tabella B-1: *Cartella* Installed Root Directory

Privilegio	Amministratore, SYSTEM	Analista, sviluppatore di metodi, revisore
Controllo completo	Consentito	—
Attraversamento cartella / Esecuzione file	Consentito	Consentito
Elenco cartelle / Lettura file	Consentito	Consentito
Lettura attributi	Consentito	Consentito
Lettura attributi estesi	Consentito	Consentito
Creazione file / Scrittura dati	Consentito	Consentito
Creazione cartelle / Aggiunta dati	Consentito	Consentito
Scrittura attributi	Consentito	Consentito
Scrittura attributi estesi	Consentito	Consentito
Eliminazione sottocartelle e file	Consentito	—
Eliminazione	Consentito	—
Lettura autorizzazioni	Consentito	Consentito
Modifica autorizzazioni	Consentito	—

Tabella B-1: *Cartella* Installed Root Directory (continua)

Privilegio	Amministratore, SYSTEM	Analista, sviluppatore di metodi, revisore
Assunzione proprietà	Consentito	—

Tabella B-2: Cartelle *`Installed Root Directory`*`\NetworkBackup` e *`Installed Root Directory`*`\TempData`

Privilegio	Amministratore, SYSTEM	Analista, sviluppatore di metodi, revisore
Controllo completo	Consentito	—
Attraversamento cartella / Esecuzione file	Consentito	Consentito
Elenco cartelle / Lettura file	Consentito	Consentito
Lettura attributi	Consentito	Consentito
Lettura attributi estesi	Consentito	Consentito
Creazione file / Scrittura dati	Consentito	Consentito
Creazione cartelle / Aggiunta dati	Consentito	Consentito
Scrittura attributi	Consentito	Consentito
Scrittura attributi estesi	Consentito	Consentito
Eliminazione sottocartelle e file	Consentito	Consentito
Eliminazione	Consentito	Consentito
Lettura autorizzazioni	Consentito	Consentito
Modifica autorizzazioni	Consentito	—
Assunzione proprietà	Consentito	—

Tabella B-3: Cartella `C:\ProgramData\SCIEX\Audit Data`

Privilegio	Amministratore, SYSTEM	Analista, sviluppatore di metodi, revisori
Controllo completo	Consentito	—
Attraversamento cartella / Esecuzione file	Consentito	Consentito
Elenco cartelle / Lettura file	Consentito	Consentito
Lettura attributi	Consentito	Consentito
Lettura attributi estesi	Consentito	Consentito
Creazione file / Scrittura dati	Consentito	Consentito
Creazione cartelle / Aggiunta dati	Consentito	Consentito
Scrittura attributi	Consentito	Consentito
Scrittura attributi estesi	Consentito	Consentito
Eliminazione sottocartelle e file	Consentito	—
Eliminazione	Consentito	—
Lettura autorizzazioni	Consentito	Consentito
Modifica autorizzazioni	Consentito	—
Assunzione proprietà	Consentito	—

Eventi di audit C

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.

Audit trail del progetto

Ogni progetto dispone di un audit trail del progetto. L'audit trail del progetto è salvato nella cartella `Audit Data` del 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 Mappa di audit muta.

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

Tabella C-1: Eventi di audit trail del progetto

SCIEX OS o CAC	Software Analyst
Area di lavoro Analisi	
Concentrazione effettiva modificata	Eventi quantificazione: **'Concentration' has been changed**
File di elaborazione automatica salvato	—
ID codice a barre modificato	—
Campione di confronto modificato nel flusso di lavoro non mirato	—
Colonne personalizzate modificate	Eventi quantificazione: **'Custom Title' has changed**
Esplorazione dati aperta	Eventi progetto: **Data File has been opened**
Dati esportati	—
Dati trasferiti a LIMS	—
Fattore di diluizione modificato	Eventi quantificazione: **'Dilution Factor' has been changed**
Calibrazione esterna modificata	—
Calibrazione esterna esportata	—
File salvato	Eventi progetto: **Quantitation Results Table has been created**, **Quantitation Results Table has been modified**, Quantitation Events: **Results Table has been saved**

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

SCIEX OS o CAC	Software Analyst
Colonna formula modificata	Eventi quantificazione: **Formula name has been changed**, **Formula name has been added**, **Formula string has been changed**, **Formula column has been removed**
Integrazione cancellata	—
Parametri di integrazione modificati	Eventi quantificazione: **Quantitation peak has been integrated**
Risultato di ricerca libreria modificato	—
Integrazione manuale	Eventi quantificazione: **Quantitation Peak has been integrated**
Integrazione manuale invertita	Eventi quantificazione: **Quantitation peak has been reverted back to original**
Selezione MS/MS modificata	—
Metodo di trattamento modificato e applicato	Eventi quantificazione: **Quantitation method has been changed**
Metodo di trattamento salvato	—
Impostazioni predefinite del progetto modificate	—
Report creato	Eventi progetto: **Printing document on printer, Finished printing document on printer**
Tabella dei risultati approvata	Eventi quantificazione: **QA reviewer has accessed a results table**
Tabella dei risultati creata	Eventi quantificazione: **Results table has been created**
Tabella dei risultati bloccata	—
Tabella dei risultati sbloccata	—
ID campione modificato	Eventi quantificazione: **'Sample ID' has been changed**
Nome campione modificato	Eventi quantificazione: **'Sample Name' has been changed**
Tipo di campione modificato	Eventi quantificazione: **'Sample Type' has been changed**

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

SCIEX OS o CAC	Software Analyst
Campioni aggiunti o rimossi	Eventi quantificazione: **Files have been added to Results Table**, **Files have been removed from Results Table**, **Samples have been added/removed**
Concentrazione effettiva aggiunta standard modificata	—
Selezione colonna Usato modificata	Eventi quantificazione: **'Use IT' has been changed**
Peso/Volume modificato	**'Weight to Volume Ratio' has been changed**
Finestra/Riquadro stampato	Eventi progetto: **Printing document on printer**, **Finished printing document on printer**
Pagina Mappa di audit	
Mappa di audit progetto modificata	Eventi progetto: **Project Settings have been changed**
Audit trail progetto esportato	—
Audit trail progetto stampato	—
Area di lavoro Lotto	
Informazioni lotto importate da LIMS/ testo	—
Lotto salvato	—
Lotto inviato	Eventi strumento: **Batch file submitted**
Stampa	Eventi progetto: **Printing Document on printer**, **Finished printing document on printer**
Area di lavoro Explorer[4]	
Apri campione/i	Eventi progetto: **Data File has been opened**
Stampa	Eventi progetto: **Printing Document on printer**, **Finished printing document on printer**
Ricalibra campione/i	—
Ricalibra campione/i avviato/i	—

[4] Gli eventi Explorer sono registrati nell'audit trail del progetto quando gli utenti utilizzano i dati nel progetto attivo.

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

SCIEX OS o CAC	Software Analyst
Area di lavoro Metodo LC	
Metodo LC salvato	—
Stampa	Eventi progetto: **Printing Document on printer**, **Finished printing document on printer**
Area di lavoro Metodo MS	
Metodo MS salvato	—
Stampa	Eventi progetto: **Printing Document on printer**, **Finished printing document on printer**
Area di lavoro Coda	
Acquisizione campione completata	—
Campione modificato	—
Acquisizione campione iniziata	—
Campione trasferito	—

Audit trail workstation

Ogni workstation dispone di un audit trail workstation. L'audit trail 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 **Mappa di audit muta**.

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

Tabella C-2: Eventi di audit trail workstation

SCIEX OS	Software Analyst
Mappa di audit	
Mappa di audit workstation modificata	Eventi strumento: **Instrument Settings have been changed**
Audit trail workstation stampato	—
Audit trail workstation esportato	—
CAC	

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

SCIEX OS	Software Analyst
Amministrazione centrale abilitata/ disabilitata	—
Impostazioni centrali recuperate/non recuperate	—
Checksum file di dati	
Checksum del file di dati wiff modificato	—
Area di lavoro Explorer[5]	
Apri campione/i	Eventi progetto: **Data File has been opened**
Stampa	Eventi progetto: **Printing document on printer**, **Finished printing document on printer**
Ricalibra campione/i	—
Ricalibra campione/i avviato/i	—
Configurazione hardware	
Dispositivi attivati	Eventi strumento: **Hardware profile has been activated**
Dispositivi disattivati	Eventi strumento: **Hardware profile has been deactivated**
Tuning strumento	
Aggiornamento tuning MS automatico	Eventi strumento: **Tune parameter settings changed**
Firmware modificato	—
Modifiche tuning MS	Eventi strumento: **Tune parameter settings changed**
Stampa risultato procedura in MS Tune	Eventi progetto: **Printing Document on printer**, **Finished printing document on printer**
Area di lavoro Coda	
Iniezione automatica effettuata	—
Reiniezione automatica effettuata	—
Lotto spostato nella coda	Eventi strumento: **Move Batch**

[5] Gli eventi Explorer sono registrati nell'audit trail della workstation quando gli utenti utilizzano i dati nel progetto attivo.

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

SCIEX OS	Software Analyst
Coda di stampa	Eventi progetto: **Printing Document on printer**, **Finished printing document on printer**
Riacquisizione campione	Eventi strumento: **Reacquiring sample(s)**
Acquisizione campione completata	Eventi progetto: **Sample has been added to Data file**
Campione modificato	—
Campione spostato nella coda	Eventi strumento: **Sample moved from position *x* to position *y* of Batch File**
Acquisizione campione iniziata	—
Security	
Disconnessione automatica da parte del sistema	Eventi strumento: **User Logged out**
Disconnessione forzata da parte di un altro utente	Eventi strumento: **User Logged out**
Disconnessione forzata non riuscita	—
Sblocco schermo non riuscito	—
Credenziali account di rete protetto modificate	Eventi strumento: **Acquisition Account Changed**
Credenziali account di rete protetto rimosse	Eventi strumento: **Acquisition Account Changed**
Credenziali account di rete protetto specificate	Eventi strumento: **Acquisition Account Changed**
Configurazione sicurezza modificata	Eventi strumento: **The Security Configuration has been modified**, **Screen Lock Changed**, **Auto Logout changed**
Utente aggiunto/eliminato	Eventi strumento: **User Added**, **User Deleted**
L'utente si è connesso	Eventi strumento: **User Logged In**
L'utente si è disconnesso	Eventi strumento: **User Logged out**
L'utente ha disattivato la modalità esclusiva	—
Accesso utente non riuscito	Eventi strumento: **User Login Failed**
Impostazioni di gestione utenti esportate	—

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

SCIEX OS	Software Analyst
Impostazioni di gestione utenti importate	—
Impostazioni di gestione utenti ripristinate	—
Ruolo utente assegnato a utente/gruppo di utenti	Eventi strumento: **User Changed User Type**
Ruolo utente eliminato	Eventi strumento: **User Type Deleted**
Ruolo utente modificato	Eventi strumento: **User Type Changed**
UserLog	
Stampa log eventi	—

Tabella C-3: Eventi di audit trail CAC

CAC	Software Analyst
Pagina Mappa di audit	
Mappa di audit workstation modificata	Eventi strumento: **Instrument Settings have been changed**
Audit trail workstation stampato	—
Audit trail workstation esportato	—
CAC	
Impostazioni CAC esportate	—
Impostazioni CAC importate	—
Impostazioni CAC ripristinate	—
Impostazioni progetto abilitate/ disabilitate in un gruppo di lavoro	—
Progetto assegnato/non assegnato a un gruppo di lavoro	—
Autorizzazione di sicurezza aggiunta per l'amministrazione centrale	—
Utente aggiunto/eliminato	—
Ruolo utente aggiunto	—
Ruolo utente eliminato	—
Ruolo utente modificato	—

Tabella C-3: Eventi di audit trail CAC (continua)

CAC	Software Analyst
Ruolo/i utente assegnati/non assegnati a utente/i nel gruppo di lavoro	—
Utente/i/Gruppo/i utenti assegnati/non assegnati a un gruppo di lavoro	—
Gruppo di lavoro aggiunto/eliminato	—
Gruppo di lavoro rinominato	—
Workstation assegnata/e/non assegnate a un gruppo di lavoro	—
Security	
Disconnessione automatica da parte del sistema	Eventi strumento: **User Logged out**
Disconnessione forzata da parte di un altro utente	Eventi strumento: **User Logged out**
Disconnessione forzata non riuscita	—
Sblocco schermo non riuscito	—
Credenziali account di rete protetto modificate	Eventi strumento: **Acquisition Account Changed**
Credenziali account di rete protetto rimosse	Eventi strumento: **Acquisition Account Changed**
Credenziali account di rete protetto specificate	Eventi strumento: **Acquisition Account Changed**
Configurazione sicurezza modificata	Eventi strumento: **The Security Configuration has been modified**, **Screen Lock Changed**, **Auto Logout changed**
Utente aggiunto/eliminato	Eventi strumento: **User Added**, **User Deleted**
L'utente si è connesso	Eventi strumento: **User Logged In**
L'utente si è disconnesso	Eventi strumento: **User Logged out**
L'utente ha disattivato la modalità esclusiva	—
Accesso utente non riuscito	Eventi strumento: **User Login Failed**
Impostazioni di gestione utenti esportate	—
Impostazioni di gestione utenti importate	—

Tabella C-3: Eventi di audit trail CAC (continua)

CAC	Software Analyst
Impostazioni di gestione utenti ripristinate	—
Ruolo utente assegnato a utente/gruppo di utenti	Eventi strumento: **User Changed User Type**
Ruolo utente eliminato	Eventi strumento: **User Type Deleted**
Ruolo utente modificato	Eventi strumento: **User Type Changed**
UserLog	
Stampa log eventi	—

Mapping di autorizzazioni tra il software SCIEX OS e Analyst

D

Questa sezione viene fornita per gli utenti che intendono eseguire la migrazione dal software Analyst al software SCIEX OS, per agevolare la migrazione delle impostazioni di sicurezza utente. Mostra le autorizzazioni nel software Analyst che corrispondono alle autorizzazioni nel software SCIEX OS.

Tabella D-1: Mapping di autorizzazioni

SCIEX OS Software	Software Analyst
Area di lavoro Lotto	
Invia metodi sbloccati	—
Apri	Lotto: **Open Existing Batches**
Salva con nome	Lotto: **Create New Batches**, **Import**, **Edit Batches**, **Save Batches**, **Overwrite Batches**
Invia	Lotto: **Submit Batches**
Salva	Lotto: **Save Batches**, **Overwrite Batches**
Salva tabella di riferimento ionica	—
Aggiungi sottocartelle dati	—
Configura regole di decisione	—
Area di lavoro Configurazione	
Scheda Generale	—
Generale: modifica impostazione regionale	—
Generale: modalità schermo intero	—
Generale: arresta i servizi Windows	—
Scheda Comunicazione LIMS	—
Scheda mappe di audit	Audit Trail Manager: **Change Audit Trail Settings**, **Create or Modify Audit Maps**
Scheda Coda	—
Coda: tempo inattività strumento	—
Coda: numero max. di campioni acquisiti	—
Coda: altre impostazioni coda	—

Tabella D-1: Mapping di autorizzazioni (continua)

SCIEX OS Software	Software Analyst
Scheda Progetti	—
Progetti: crea progetto	Applicazione Analyst: **Create Project**
Progetti: applica un modello mappa di audit a un progetto esistente	Audit Trail Manager: **Change Audit Trail Settings**
Progetti: crea directory radice	Applicazione Analyst: **Create Root Directory**
Progetto: imposta directory radice corrente	Applicazione Analyst: **Set Root Directory**
Progetti: specifica credenziali di rete	—
Progetti: abilita scrittura checksum per creazione dati wiff	—
Progetti: cancella directory radice	—
Scheda Dispositivi	Configurazione hardware: **Create**, **Delete**, **Edit**, **Activate/Deactivate**
Scheda Gestione utenti	**Security Config**
Forza disconnessione utente	**Unlock/Logout Application**
Scheda CAC[3]	—
Scheda Modelli di stampa	—
Modelli di stampa: crea e modifica modelli di stampa	—
Modelli di stampa: imposta modello di stampa predefinito	—
Modelli di stampa: applica il modello corrente a tutti i progetti nella directory radice	
Area di lavoro Log eventi	
Accedi all'area di lavoro log eventi	—
Archivia log	—
Area di lavoro Audit trail	
Accedi all'area di lavoro audit trail	Audit Trail Manager: **View Audit Trail Data**
Visualizza mappa di audit attiva	Audit Trail Manager: **View Audit Trail Data**

[3] Nella versione 3.1, l'autorizzazione **Abilita amministrazione centrale** è stata rinominata in **CAC**. La pagina CAC nell'area di lavoro Configurazione consente di configurare l'amministrazione centrale del software SCIEX OS.

Tabella D-1: Mapping di autorizzazioni (continua)

SCIEX OS Software	Software Analyst
Stampa/Esporta audit trail	Audit Trail Manager: **View Audit Trail Data**
Data Acquisition Panel	
Inizio	—
Interrompi	—
Salva	—
Aree di lavoro Metodo MS e Metodo LC	
Accedi all'area di lavoro metodo	—
Nuovo	Metodo di acquisizione: **Create/Save acquisition method**
Apri	Metodo di acquisizione: **Open acquisition method as read-only (acquire mode)**
Salva	Metodo di acquisizione: **Overwrite acquisition methods**, **Create/Save acquisition method**
Salva con nome	Metodo di acquisizione: **Overwrite acquisition methods**, **Create/Save acquisition method**
Blocca/Sblocca metodo	—
Area di lavoro Coda	
Gestisci	Coda campioni: **Reacquire**, **Delete Sample or Batch**, **Move Batch**
Avvia/Arresta	Coda campioni: **Start Sample**, **Stop Sample**, **Abort Sample**, **Stop Queue**
Stampa	Editor modello di report: **Print**
Modifica campione	—
Area di lavoro Libreria	
Accedi all'area di lavoro libreria	Esplora: **Setup library location**, **Setup library user options**, **Add library record**, **Add spectrum to library**, **Modify library record (overrides add/delete if disabled)**, **Delete MS spectrum**, **Delete UV spectrum**, **Delete structure**, **View library**, **Search library**
Area di lavoro MS Tune	
Accedi all'area di lavoro MS Tune	—

Tabella D-1: Mapping di autorizzazioni (continua)

SCIEX OS Software	Software Analyst
Tuning MS avanzato	Tuning: **Instrument Optimization**, **Manual Tune**, **Edit Tuning Options**
Risoluzione dei problemi avanzata	—
Controllo stato rapido	Tuning: **Instrument Opt**
Ripristina dati strumento	Tuning: **Edit Tuning Options**, **Edit instrument data**
Area di lavoro Explorer	
Accedi all'area di lavoro Explorer	—
Esporta	Esplora: **Save data to text file**
Stampa	Editor modello di report: **Print**
Opzioni	—
Ricalibra	Tuning: **Calibrate from current spectrum**
Area di lavoro Analisi	
Nuovi risultati	Quantificazione: **Create new results tables**
Crea metodo di elaborazione	Quantificazione: **Create quantitation methods**
Modifica metodo di elaborazione	Quantificazione: **Modify existing methods**
Consenti l'esportazione e la creazione del report della tabella dei risultati sbloccata	—
Salva risultati per lotto automazione	—
Modifica algoritmo di integrazione metodo di quantificazione predefinito	Quantificazione: **Change default method options**
Modifica parametri di integrazione metodo di quantificazione predefinito	Quantificazione: **Change default method options**
Abilita avviso picco modificato progetto	—
Aggiungi campioni	Quantificazione: **Add and Remove samples from results table**
Rimuovi campioni selezionati	Quantificazione: **Add and Remove samples from results table**
Esporta, importa o rimuovi calibrazione esterna	—
Modifica nome campione	Quantificazione: **Modify sample name**
Modifica tipo di campione	Quantificazione: **Modify Sample Type**

Tabella D-1: Mapping di autorizzazioni (continua)

SCIEX OS Software	Software Analyst
Modifica ID campione	Quantificazione: **Modify Sample ID**
Modifica concentrazione effettiva	Quantificazione: **Modify Analyte Concentration**
Modifica fattore di diluizione	Quantificazione: **Modify Dilution Factor**
Modifica campi commento	Quantificazione: **Modify Sample Comment**
Abilita integrazione manuale	Quantificazione: **Manually integrate**
Imposta picco su non trovato	—
Includi o escludi un picco dalla tabella dei risultati	Quantificazione: **Exclude standards from calibration**
Opzioni di regressione	Quantificazione: **Change regression parameters**
Modifica parametri di integrazione tabella dei risultati per un singolo cromatogramma	Quantificazione: **Change "simple" parameters in peak review, Change "advanced" parameters in peak review**
Modifica metodo di quantificazione per componente tabella dei risultati	Quantificazione: **Edit results tables' method**
Crea nuove impostazioni tracciato metrico	Quantificazione: **Modify or create metric plot settings**
Aggiungi colonne personalizzate	Quantificazione: **Create or modify formula columns**
Imposta formato titolo verifica picco	—
Rimuovi colonna personalizzata	Quantificazione: **Create or modify formula columns**
Impostazioni di visualizzazione tabella dei risultati	Quantificazione: **Change results table column precision**, **Change results table column visibility**, **Modify results table settings**
Blocca tabella dei risultati	—
Sblocca tabella dei risultati	—
Contrassegna file dei risultati come rivisto e salva	—
Modifica modello report	Editor modello di report: **Create/Modify report templates**
Trasferisci risultati a LIMS	—
Modifica colonna codice a barre	—

Tabella D-1: Mapping di autorizzazioni (continua)

SCIEX OS Software	Software Analyst
Modifica assegnazione campione di confronto	—
Aggiungi gli spettri MSMS alla libreria	Esplora: **Add spectrum to library record**
Impostazioni predefinite progetto	Quantificazione: **Modify global (default) settings**
Crea report in tutti i formati	—
Modifica parametri criteri di segnalazione	—
Modifica parametro di rimozione automatica anomalie	—
Abilita rimozione automatica anomalie	—
Aggiorna metodo di trattamento tramite FF/LS	—
Aggiorna risultati tramite FF/LS	—
Abilita funzionalità di raggruppamento per addotti	Quantificazione: **Create Analyte Groups**, **Modify Analyte Groups**
Cerca file	—
Abilita aggiunta standard	—
Imposta regola percentuale di integrazione manuale	Quantificazione: **Enable or Disable percent rule in Manual Integration**
Modifica peso/volume	Quantificazione: **Modify Weight To Volume ratio**

Data File Checksum E

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 Configurazione.
2. Fare clic su **Progetti**.
3. Se richiesto, espandere **Sicurezza file di dati**.
4. Per abilitare la funzione Data File Checksum, selezionare la casella di controllo **Abilita scrittura del checksum per la creazione di dati wiff**. 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 questo documento in formato elettronico, è necessario 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 del prodotto hardware, fare riferimento alla documentazione fornita con il sistema o il 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.