SCIEX
The Power of Precision

SCIEX OS Software

Handbuch für Laborleiter

RUO-IDV-05-7370-DE-L

August 2023

Nur für Forschungszwecke. Nicht zur Verwendung bei Diagnoseverfahren.

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

Inhalt

Einleitung 1

Die in diesem Handbuch enthaltenen Informationen richten sich an zwei primäre Zielgruppen:

- Den Laborleiter, der sich mit dem täglichen Betrieb und der Nutzung der SCIEX OS Software und den dazu gehörenden Instrumenten aus funktionaler Sicht befasst.
- Systemadministratoren, die sich mit der Sicherheit des Systems und mit der System- und Datenintegrität befassen.

Übersicht über die Sicherheitskonfiguration 2

In diesem Abschnitt wird beschrieben, wie die Komponenten für Zugriffskontrolle und Auditing in der SCIEX OS Software in Verbindung mit den Windows-Komponenten für Zugriffskontrolle und Auditing arbeiten. Außerdem wird die Konfiguration der Windows-Sicherheit vor der Installation der SCIEX OS Software beschrieben.

Sicherheit und Einhaltung gesetzlicher Vorschriften

Die SCIEX OS Software umfasst Folgendes:

- Anpassbare Verwaltung, um den Bedürfnissen von Forschung und regulatorischen Anforderungen gerecht zu werden.
- Sicherheits- und Prüfwerkzeuge für die Unterstützung der Konformität nach 21 CFR Part 11 für die Verwendung von elektronischen Aufzeichnungen.
- Flexible und effiziente Verwaltung des Zugangs zu kritischen Massenspektrometer-Funktionen.
- Kontrollierter und geprüfter Zugriff auf wichtige Daten und Berichte.
- Einfache Sicherheits-Management-Anbindung an Windows-Sicherheit.

Sicherheitsanforderungen

Die Sicherheitsanforderungen reichen von relativ offenen Umgebungen wie in Forschungs- oder akademischen Labors bis hin zu extrem streng geregelten Umgebungen wie jene in forensischen Labors.

SCIEX OS Software und „Windows Security“: Zusammenarbeit

Die SCIEX OS Software und das Windows New Technology File System (NTFS) verfügen über Sicherheitsfunktionen für die Steuerung des System- und Datenzugriffs.

Die Windows-Sicherheit bietet die erste Schutzebene, indem von Nutzern verlangt wird, sich am Netzwerk mit einem eindeutigen Benutzernamen und Passwort anzumelden. Das führt dazu, dass nur Benutzer, die von den lokalen Windows-Sicherheitseinstellungen oder von den Windows-Netzwerkeinstellungen erkannt werden, Zugriff auf das System erhalten. Weitere Informationen finden Sie im Abschnitt: Windows-Sicherheitskonfiguration.

Die SCIEX OS Software hat die folgenden Zugriffsmodi auf das Sicherheitssystem:

- „Mixed Mode“ (Gemischter Modus)

- „Integrated Mode“ (Integrierter Modus) (Standardeinstellung)

Weitere Informationen über Sicherheitsmodi und Sicherheitseinstellungen finden Sie im Abschnitt: Konfigurieren des Sicherheitsmodus.

SCIEX OS bietet zudem vollständig konfigurierbare Rollen, die von den mit Windows verbundenen Benutzergruppen getrennt sind. Durch die Verwendung von Rollen kann der Laborleiter den Zugriff auf die Software und das Massenspektrometer auf der Grundlage der Funktion steuern. Weitere Informationen finden Sie im Abschnitt: Konfiguration des Zugriffs auf die SCIEX OS Software.

Audit-Trails innerhalb der SCIEX OS Software und Windows

Die Auditing-Funktionen in der SCIEX OS-Software, zusammen mit den integrierten Windows-Auditing-Komponenten, sind für die Erstellung und Verwaltung von elektronischen Aufzeichnungen entscheidend.

SCIEX OS bietet ein System von Audit-Trails, das die Anforderungen an elektronische Aufzeichnungen erfüllt. Separate Audit-Trail-Aufzeichnungen:

- Änderungen von Massenkalibrierungstabellen oder Auflösungstabellen, Änderungen der Systemkonfiguration und sicherheitsrelevante Ereignisse.
- Erstellungs- und Änderungsereignisse für Projekte, Tuning, Batches, Daten, Verarbeitungsmethoden und Berichtvorlagendateien sowie das Öffnen und Schließen von Modulen und Druckereignisse. Zu den Löschereignissen, die im Audit-Trail aufgezeichnet werden, gehören das Löschen von Rollen und Benutzern in der SCIEX OS Software.
- Erstellung und Änderung der Probeninformationen, Peak-Integrations-Parameter und integrierten Verarbeitungsmethode in einer Ergebnistabelle.

Eine vollständige Liste der Audit-Ereignisse finden Sie im Abschnitt: Audit-Ereignisse.

Die SCIEX OS-Software verwendet Folgendes: Anwendungsereignisprotokoll, um Informationen über den Betrieb der Software zu erfassen. Verwenden Sie dieses Protokoll als Hilfe bei der Fehlerbehebung. Es beinhaltet detaillierte Informationen über Interaktionen von Massenspektrometer, Geräten und Software.

Windows verwaltet Ereignisprotokolle, die eine Reihe von Sicherheits-, System- und anwendungsspezifischen Ereignissen erfassen. In den meisten Fällen ist die Windows-Überwachung so ausgelegt, dass außergewöhnliche Ereignisse erfasst werden, wie beispielsweise ein Fehler beim Anmelden. Der Administrator kann das System so konfigurieren, dass eine breite Palette von Ereignissen erfasst wird, wie z. B. der Zugriff auf bestimmte Dateien oder administrative Tätigkeiten unter Windows. Weitere Informationen finden Sie im Abschnitt: System-Audits.

Sicherheitsrichtlinien für Kunden: Sicherungen

Die Sicherung der Kundendaten liegt in der Verantwortung des Kunden. SCIEX Service- und Support-Mitarbeiter stehen für Ratschläge und Empfehlungen bezüglich der Sicherung der Kundendaten zur Verfügung, es liegt jedoch in der Verantwortung des Kunden, sicherzustellen, dass die Daten entsprechend den Richtlinien, Anforderungen und den

gesetzlichen Anforderungen des Kunden gesichert werden. Häufigkeit und Umfang der Sicherung der Kundendaten sollte den organisatorischen Anforderungen und der Kritikalität der generierten Daten entsprechen.

Kunden sollten sicherstellen, dass die Sicherungen fehlerfrei funktionieren, da Sicherungen ein wesentlicher Bestandteil der gesamten Datenverwaltung und wichtig für die Wiederherstellung im Falle eines böswilligen Angriffs, Hardwarefehlers oder Softwarefehlers sind. Erstellen Sie keine Sicherungen während der Datenerfassung oder stellen Sie sicher, dass die Daten, die gerade erfasst werden, von der Sicherungssoftware ignoriert werden. Es wird dringend empfohlen, eine vollständige Sicherung des Computers vorzunehmen, bevor Sicherheits-Updates installiert oder Reparaturen am Computer durchgeführt werden. Dies vereinfacht ein Rollback in dem seltenen Fall, dass sich ein Sicherheitspatch auf die Funktionsfähigkeit einer Anwendung auswirkt.

21 CFR Teil 11

Die SCIEX OS-Software enthält die technischen Kontrollen zur Unterstützung von 21 CFR Teil 11 durch folgende Implementierungen:

- Verknüpfung der Sicherheit der Modi „Mixed“ (gemischt) und „Integrated“ (integriert) mit der Windows-Sicherheit
- Kontrollierter Zugriff auf Funktionen über anpassbare Rollen
- Audit-Trails für den Gerätebetrieb, die Datenerfassung, Datenprüfung und Berichterstellung
- Elektronische Signaturen aus einer Kombination von Benutzer-ID und Passwort
- Die ordnungsgemäße Konfiguration des Windows-Betriebssystems
- Ordnungsgemäße Verfahren und Schulungen innerhalb des Unternehmens

Die SCIEX OS-Software wurde als Teil eines mit 21 CFR Teil 11 konformen Systems entwickelt und kann für die Unterstützung der Konformität mit 21 CFR Teil 11 konfiguriert werden. Ob die Nutzung der SCIEX OS-Software mit 21 CFR Teil 11 konform ist oder nicht, hängt von der Nutzung der optionalen SCIEX OS CFR-Lizenz und der Konfiguration der SCIEX OS-Software ab. Erforderliche Richtlinien und Verfahren sowie die damit verbundenen Schulungsanforderungen müssen im Labor ebenfalls umgesetzt werden.

Validierungsdienste stehen über SCIEX Professional Services zur Verfügung. Für weitere Informationen kontaktieren Sie complianceservices@sciex.com.

Hinweis: Belassen Sie die Instrument Settings Converter Software nicht auf einem validierten System. Sie ist vorgesehen für die erste Übertragung der Geräteeinstellungen von Analyst zur SCIEX OS-Software. Stellen Sie sicher, dass die Instrument Settings Converter-Software vom Computer entfernt wird, nachdem sie verwendet wurde.

Systemkonfiguration

Die Systemkonfiguration wird in der Regel durch Netzwerkadministratoren oder Personen mit Netzwerk- und lokalen Administrationsrechten durchgeführt.

Windows-Sicherheitskonfiguration

Dieser Abschnitt enthält Richtlinien für die Konfiguration von Windows:

- Befolgen Sie diese Richtlinien für Windows-Konten und -Passwörter:
  - Das Windows-Passwort muss alle 90 Tage geändert werden.
  - Das Windows-Passwort kann für mindestens eine folgende Iteration nicht mehr verwendet werden. Das bedeutet, dass das neue Passwort nicht das unmittelbar vorhergehende Passwort sein darf.
  - Das Windows-Passwort muss mindestens acht Zeichen umfassen.
  - Das Windows-Passwort muss mindestens zwei der folgenden Anforderungen erfüllen, um den Komplexitätsvorgaben zu entsprechen:
    - Ein Buchstabe in Großschreibung
    - Ein Buchstabe in Kleinschreibung
    - Ein numerischer Wert
    - Ein Sonderzeichen (wie beispielsweise: ! @ # $ % ^ &)
  - Der Windows-Benutzername darf nicht **Admin**, **Administrator** oder **Demo** sein.
- Stellen Sie sicher, dass der Administrator der SCIEX OS Software die Möglichkeit hat, Dateiberechtigungen für den Ordner `SCIEX OS Data` zu ändern. Wenn sich dieser Ordner auf einem lokalen Computer befindet, empfiehlt es sich, dass der Software-Administrator Teil der lokalen Administratoren-Gruppe ist.
- Um sicherzustellen, dass für die Netzwerkerfassung alle Benutzer über den erforderlichen Zugriff auf die Ressourcen verfügen, muss der Netzwerk-Administrator ein sicheres Netzwerkkonto (SNA) für die Netzwerkressource hinzufügen. Dieses Konto muss über Schreibzugriff für den Netzwerkordner verfügen, der das Stammverzeichnis enthält. Es wird in den Eigenschaften des Stammverzeichnisses als sicheres Netzwerkkonto (SNA) festgelegt.

Hinweis: Es wird empfohlen, Bibliotheksdateien von einer lokalen Festplatte zu importieren.

Hinweis: Informationen über die für verschiedene Benutzerrollen erforderlichen Windows-Berechtigungen finden Sie im Abschnitt: Windows-Berechtigungen.

Benutzer und Gruppen

Die SCIEX OS-Software verwendet die Benutzernamen und Passwörter, die in der „Primary Domain Controller Security“-Datenbank oder in Active Directory erfasst sind. Passwörter werden mit den von Windows zur Verfügung gestellten Tools verwaltet. Für weitere Informationen über das Hinzufügen und Konfigurieren von Personen und Rollen siehe Abschnitt: Konfiguration des Zugriffs auf die SCIEX OS Software.

Unterstützung von Active Directory

Beim Hinzufügen von Benutzern im Arbeitsbereich „Konfiguration“ von SCIEX OS geben Sie die Benutzerkonten im UPN-Format (User Principal Name) an. Die folgenden Versionen von Active Directory werden unterstützt:

- Windows 2012 Server
- Windows 7, 64-Bit-Clients
- Windows 10, 64-Bit-Clients

Windows-Dateisystem

In der SCIEX OS-Software müssen sich die Dateien und Verzeichnisse auf einer Festplattenpartition im NTFS-Format befinden, die den Zugriff auf die SCIEX OS-Softwaredateien steuern und überwachen kann. Das FAT-Dateisystem (FAT = File Allocation Table) kann den Zugriff auf Ordner oder Dateien nicht steuern oder überwachen und ist daher für eine sichere Umgebung nicht geeignet.

Datei- und Ordnerberechtigungen

Zur Verwaltung der Sicherheit muss der Administrator der SCIEX OS Software das Recht haben, Berechtigungen für den Ordner `SCIEX OS Data` zu ändern. Der Zugang muss durch den Netzwerkadministrator eingerichtet werden.

Hinweis: Beziehen Sie dabei den Grad des Zugriffs, den die Benutzer auf das Laufwerk, das Stammverzeichnis und die Projektordner auf den einzelnen Computern benötigen, in die Überlegungen mit ein. Konfigurieren Sie Sharing (gemeinsame Nutzung) und die damit verbundenen Berechtigungen. Weitere Informationen über File-Sharing finden Sie in der Windows-Dokumentation.

Hinweis: Um Probleme mit Berechtigungen zu vermeiden, empfiehlt es sich, Bibliotheksdateien von einer lokalen Festplatte zu importieren.

Hinweis: Informationen über die für verschiedene Benutzerrollen erforderlichen Windows-Berechtigungen finden Sie im Abschnitt: Windows-Berechtigungen.

Informationen über Datei- und Ordner-Berechtigungen in der SCIEX OS Software finden Sie im Abschnitt: Zugriffssteuerung.

System-Audits

Die Überwachungsfunktion von Windows kann aktiviert werden, um Sicherheitsverletzungen oder Systemeinbrüche festzustellen. Die Auditierung (Überwachung) kann so eingestellt werden, dass verschiedene Arten von systembezogenen Ereignissen aufgezeichnet werden. Beispielsweise kann die Überwachungsfunktion aktiviert werden, um fehlgeschlagene oder erfolgreiche Anmeldeversuche im System im Ereignisprotokoll aufzuzeichnen.

Ereignisprotokolle

Der Windows Event Viewer zeichnet die überwachten Ereignisse im Sicherheits-, System- oder Anwendungsprotokoll auf.

Passen Sie die Ereignisprotokolle wie folgt an:

- Konfigurieren Sie eine geeignete Größe für das Ereignisprotokoll.
- Aktivieren Sie das automatische Überschreiben von alten Ereignissen.
- Aktivieren Sie die Windows-Sicherheitseinstellungen.

Es kann ein Prozess für die Überprüfung und Speicherung eingerichtet werden. Weitere Informationen über Sicherheitseinstellungen und Überwachungsrichtlinien finden Sie in der Windows-Dokumentation.

Windows-Benachrichtigungen

Für den Fall, dass ein System- oder Benutzerproblem auftritt, konfigurieren Sie das Netzwerk so, dass es eine automatische Nachricht an eine bestimmte Person, z. B. den Systemadministrator, auf dem gleichen oder einem anderen Computer sendet.

- Starten Sie auf dem versendenden wie auch auf dem empfangenden Computer den Benachrichtigungsdienst unter „Services“ in der Windows-Systemsteuerung.
- Starten Sie auf dem versendenden Computer den Benachrichtigungsdienst unter „Services“ (Dienste) in der Windows-Systemsteuerung.

Weitere Informationen über das Erstellen eines Benachrichtigungsobjekts finden Sie in der Windows-Dokumentation.

Elektronische Lizenzierung 3

Bei der SCIEX OS Software kann die elektronische Lizenzierung knotengebunden oder serverbasiert sein.

Für die Central Administrator Console (CAC) Software sind ausschließlich knotengebundene Lizenzen verfügbar.

Die Aktivierungs-ID wird möglicherweise für zukünftigen Service oder im Fall von Supportanfragen benötigt. Zugriff auf die Aktivierungs-ID einer knoten- oder serverbasierten Lizenz:

- Klicken Sie im Arbeitsbereich „Configuration“ im SCIEX OS-Fenster auf **Lizenzen**.

Hinweis: Stellen Sie sicher, dass Sie die Lizenz verlängern, bevor sie abläuft. Bei der Lizenz für die CAC Software handelt es sich um eine Jahreslizenz.

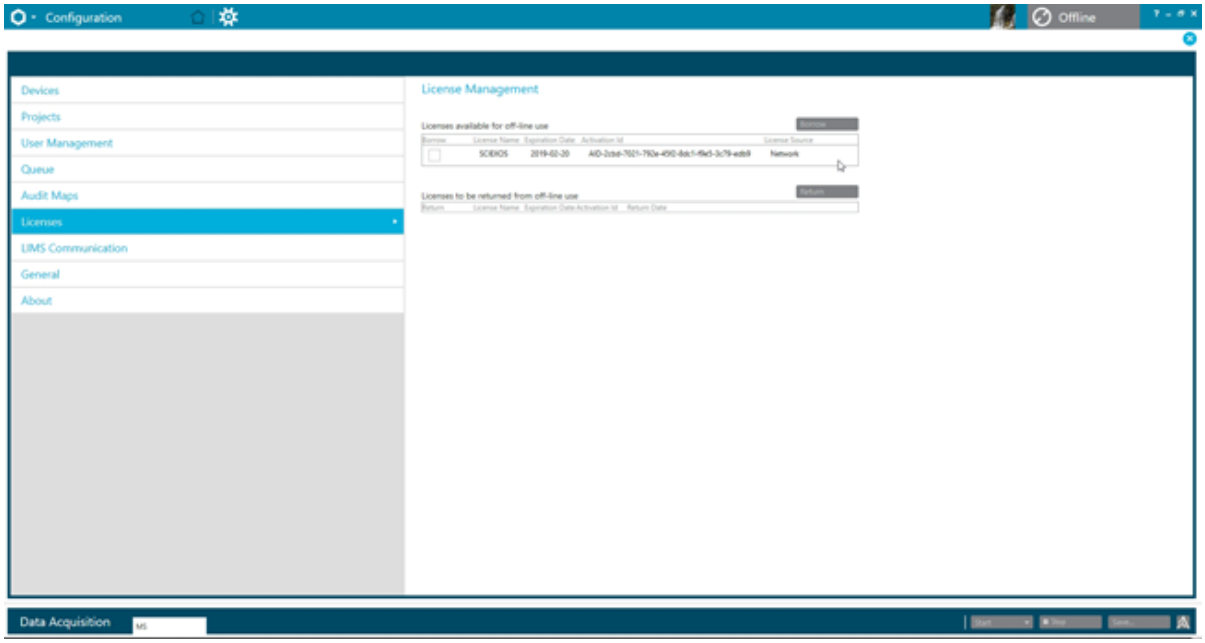
Ausleihen einer serverbasierten elektronischen Lizenz

Für die Verwendung von SCIEX OS ist eine Lizenz erforderlich. Wenn die serverbasierte Lizenzierung zum Einsatz kommt, können Benutzer, die offline arbeiten möchten, für die Dauer von bis zu 7 Tagen eine Lizenz reservieren. Während dieser Zeit ist die ausgeliehene elektronische Lizenz für den Computer reserviert.

Hinweis: Dieses Verfahren gilt nicht für die Central Administrator Console (CAC) Software.

1. Öffnen Sie den Arbeitsbereich „Konfiguration“.
2. Klicken Sie auf **Lizenzen**.
   Die Tabelle „Lizenzen für die Offline-Nutzung“ zeigt alle für das Ausleihen verfügbare Lizenzen an.

Abbildung 3-1: Lizenzmanagement: Ausleihen einer Lizenz



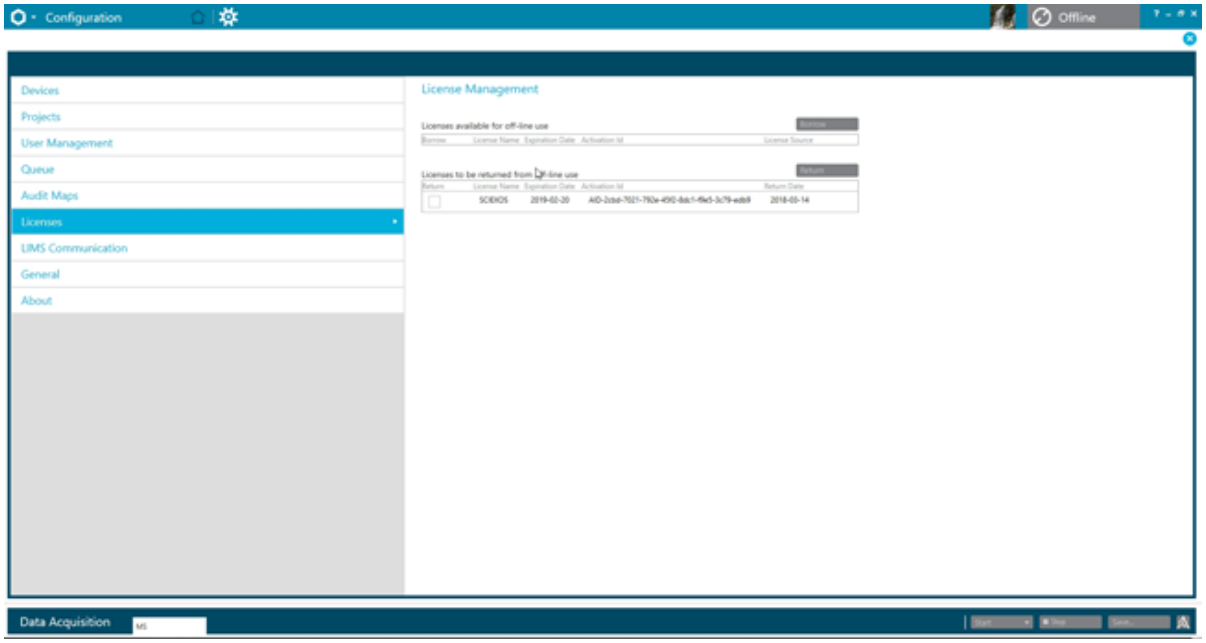
3. Wählen Sie die auszuleihende Lizenz aus und klicken Sie dann auf **Ausleihen**.

Zurückgeben einer serverbasierten elektronischen Lizenz

Hinweis: Dieses Verfahren gilt nicht für die Central Administrator Console (CAC) Software.

1. Öffnen Sie den Arbeitsbereich „Konfiguration“.
2. Klicken Sie auf **Lizenzen**.
   Die Tabelle „Von der Offline-Nutzung zurückzugebende Lizenzen“ zeigt alle Lizenzen, die zurückgegeben werden können, d. h. alle Lizenzen, die von diesem Computer ausgeliehen wurden.

Abbildung 3-2: Lizenzmanagement: Zurückgeben einer Lizenz



3. Wählen Sie die zurückzugebende Lizenz aus und klicken Sie dann auf **Zurückgeben**.

Zugriffssteuerung 4

In diesem Abschnitt wird die Steuerung des Zugriffs auf die SCIEX OS-Software beschrieben. Um den Zugriff auf die Software zu steuern, führt der Administrator die folgenden Aufgaben aus:

Hinweis: Um die Aufgaben in diesem Abschnitt ausführen zu können, muss der Benutzer über lokale Administratorrechte für die Workstation verfügen, auf der die Software installiert wird.

- Installieren und Konfigurieren der SCIEX OS-Software.
- Hinzufügen und Konfigurieren von Benutzern und Rollen
- Konfiguration des Zugriffs auf die Projekte und Projektdateien im Stammverzeichnis

Dieses Verfahren bietet Anweisungen für die lokale Verwaltung der SCIEX OS Software. Informationen über die zentrale Verwaltung der SCIEX OS Software finden Sie im Abschnitt: Central Administrator Console.

Hinweis: Änderungen der SCIEX OS-Konfiguration werden nach dem Neustart von SCIEX OS wirksam.

Speicherplatz der sicherheitsrelevanten Informationen

Alle Sicherheitsinformationen werden auf dem lokalen Computer im Ordner `C:\ProgramData\SCIEX\Clearcore2.Acquisition` in einer Datei namens `Security.data` gespeichert.

Arbeitsablauf für die Software-Sicherheit

Die SCIEX OS Software arbeitet mit den Sicherheits-, Anwendungs- und System-Ereignisüberwachungs-Komponenten der Windows Administrative Tools zusammen.

Die Sicherheit muss auf den folgenden Ebenen konfiguriert werden:

- Windows-Authentifizierung: Zugriff auf den Computer.
- Windows-Autorisierung: Zugriff auf Dateien und Ordner.
- SCIEX OS Software-Authentifizierung: Die Möglichkeit, SCIEX OS zu öffnen.
- SCIEX OS Software-Autorisierung: Zugriff auf die Funktionen in SCIEX OS.

Für eine Liste der Aufgaben im Rahmen der Sicherheitskonfiguration siehe die Tabelle: Tabelle 4-1. Für Optionen bei der Einstellung der verschiedenen Sicherheitsebenen siehe die Tabelle: Tabelle 4-2.

Tabelle 4-1: Arbeitsablauf zum Konfigurieren der Sicherheit

Aufgabe	Verfahren
Installation der SCIEX OS-Software.	Siehe das Dokument: *SCIEX OS Software-Installationshandbuch*.
Konfigurieren des Zugriffs auf die SCIEX OS Software.	Siehe Abschnitt: Konfiguration des Zugriffs auf die SCIEX OS Software.
Konfiguration der Windows-Dateisicherheit und NTFS	Siehe Abschnitt: Konfigurieren des Zugriffs auf Projekte und Projektdateien.

Tabelle 4-2: Optionen bei der Sicherheitskonfiguration

Option	CFR 21 Teil 11
Windows-Sicherheit	
Konfiguration von Benutzern und Gruppen (Authentifizierung)	Ja
Aktivierung der Windows-Überwachung sowie der Datei- und Verzeichnisüberwachung	Ja
Einstellung von Dateiberechtigungen (Autorisierung)	Ja
SCIEX OS Software-Installation	
Installation der SCIEX OS-Software.	Ja
Öffnen des Event Viewers zur Installationsprüfung	Ja
Software-Sicherheit	
Auswählen des Sicherheitsmodus	Ja
Konfigurieren der Benutzer und Rollen in der SCIEX OS Software.	Ja
Konfiguration von E-Mail-Benachrichtigungen	Ja
Erstellen von Audit-Map-Vorlagen, Konfigurieren von Audit-Trail-Maps für Projekte und Workstations	Ja
Aktivieren der Prüfsummen-Funktion für `wiff`-Dateien.	Ja
Allgemeine Aufgaben	
Hinzufügen neuer Projekte	Ja

Installieren der SCIEX OS-Software

Lesen Sie vor der Installation der SCIEX OS Software diese Dokumente, die auf der Softwareinstallations-DVD oder im Web-Download-Paket verfügbar sind: *Software-Installationshandbuch* und *Versionshinweise*. Stellen Sie sicher, dass Sie den Unterschied zwischen einem Verarbeitungscomputer und einem Erfassungscomputer kennen. Führen Sie dann die entsprechende Installation durch.

Systemvoraussetzungen

Angaben zu den Mindestanforderungen für die Installation finden Sie im Dokument: *Software-Installationshandbuch*.

Voreingestellte Auditing-Optionen

Für eine Beschreibung der installierten Audit-Maps siehe Abschnitt: Installierte Audit-Map-Vorlagen. Nach der Installation kann der Administrator der SCIEX OS Software benutzerdefinierte Audit-Maps erstellen und im Arbeitsbereich „Konfiguration“ eine andere Audit-Map zuweisen.

Konfigurieren des Sicherheitsmodus

In diesem Abschnitt werden die Optionen des „Sicherheitsmodus“ beschrieben, die auf der Seite „Benutzerverwaltung“ im Arbeitsbereich „Konfiguration“ enthalten sind.

Integrated Mode: Wenn der aktuell unter Windows angemeldete Benutzer als Benutzer in der Software definiert ist, dann hat dieser Benutzer Zugriff auf die SCIEX OS software.

Mixed Mode: Benutzer melden sich bei Windows und der Software separat an. Die für die Anmeldung bei Windows verwendeten Anmeldedaten müssen nicht mit den Anmeldedaten für SCIEX OS übereinstimmen. Verwenden Sie diesen Modus, um einer Benutzergruppe die Anmeldung bei Windows mit den gleichen Anmeldeinformationen zu ermöglichen. Für die Anmeldung bei der Software benötigt jeder Benutzer jedoch eindeutige Anmeldedaten. Diesen eindeutigen Anmeldedaten können bestimmte Rollen in der gleichen Art und Weise wie im „Integrated Mode“ zugewiesen werden.

Wenn der „Mixed Mode“ ausgewählt ist, stehen die Funktionen „Screen Lock“ und „Auto Logoff“ zur Verfügung.

Screen Lock and Auto Logoff: Aus Sicherheitsgründen kann der Computerbildschirm nach Ablauf einer bestimmten Zeit der Inaktivität gesperrt werden. Es kann zudem ein automatischer Logoff-Timer definiert werden, sodass die Software geschlossen wird, nachdem sie eine bestimmte Zeit gesperrt war. „Screen Lock“ und „Auto Logoff“ sind nur im „Mixed Mode“ verfügbar.

Hinweis: Wenn der Bildschirm gesperrt wird, werden die Erfassung und Verarbeitung fortgesetzt. Eine automatische Abmeldung erfolgt nicht, wenn die Verarbeitung erfolgt oder die Ergebnistabelle nicht gespeichert wurde. Wenn der Benutzer mit einer erzwungenen Abmeldung abgemeldet wird, dann werden alle Verarbeitungsvorgänge gestoppt und nicht gespeicherte Daten gehen verloren. Die Erfassung wird fortgesetzt, nachdem der Benutzer automatisch oder manuell abgemeldet wurde.

Security Notification: Die Software kann so konfiguriert werden, dass eine E-Mail-Benachrichtigung nach einer konfigurierbaren Anzahl von Anmeldefehlern innerhalb eines definierbaren Zeitraums automatisch gesendet wird, um vor Zugriffen auf das System durch nicht autorisierte Benutzer zu warnen. Die Anzahl der Anmeldefehler kann zwischen 3 und 7 betragen und der Zeitraum zwischen 5 Minuten und 24 Stunden.

Hinweis: Für Arbeitsgruppen, die mithilfe der Central Administrator Console (CAC)-Software verwaltet werden, kann der Sicherheitsmodus nicht mit der SCIEX OS Software verwaltet werden.

Auswählen des Sicherheitsmodus

1. Öffnen Sie den Arbeitsbereich „Konfiguration“.
2. Klicken Sie auf **Benutzerverwaltung**.
3. Klicken Sie auf die Registerkarte **Sicherheitsmodus**.
4. Wählen Sie **Integrierter Modus** oder **Gemischter Modus** aus. Siehe Abschnitt: Konfigurieren des Sicherheitsmodus.
5. Klicken Sie auf **Speichern**.
   Ein Bestätigungsdialogfeld wird angezeigt.
6. Klicken Sie auf **OK**.

Konfigurieren der Workstation-Sicherheitsoptionen (Mixed Mode)

Voraussetzungen
• Stellen Sie den Sicherheitsmodus auf „Mixed Mode“ ein. Siehe Abschnitt: Konfigurieren des Sicherheitsmodus.

Wenn der „Mixed Mode“ ausgewählt ist, dann können die Funktionen „Screen Lock“ und „Auto Logoff“ konfiguriert werden.

1. Öffnen Sie den Arbeitsbereich „Konfiguration“.
2. Klicken Sie auf **Benutzerverwaltung**.
3. Öffnen Sie die Registerkarte Sicherheitsmodus.
4. Um die Funktion „Screen Lock“ zu konfigurieren, gehen Sie wie folgt vor:
   a. Wählen Sie **Bildschirmsperre** aus.
   b. Geben Sie im Feld **Warten** eine Zeit in Minuten an.
      Wenn die Workstation für diese Zeitdauer inaktiv ist, dann wird sie automatisch gesperrt. Der angemeldete Benutzer kann die Workstation entsperren, indem er die korrekten Anmeldedaten eingibt, oder der Administrator kann den Benutzer abmelden.
5. Um die Funktion „Auto Logoff“ zu konfigurieren, gehen Sie wie folgt vor:
   a. Wählen Sie **Automatische Abmeldung** aus.
   b. Geben Sie im Feld **Warten** eine Zeit in Minuten an. Wenn die Workstation für diese Zeitdauer automatisch oder manuell gesperrt wird, dann wird der aktuell

angemeldete Benutzer abgemeldet. Alle Verarbeitungsvorgänge werden gestoppt. Die Erfassung wird jedoch fortgesetzt.

6. Klicken Sie auf **Speichern**.
   Ein Bestätigungsdialogfeld wird geöffnet.
7. Klicken Sie auf **OK**.

Konfigurieren der E-Mail-Benachrichtigung (Mixed Mode)

Voraussetzungen
• Stellen Sie den Sicherheitsmodus auf „Mixed Mode“ ein. Siehe Abschnitt: Konfigurieren des Sicherheitsmodus.

Die Software kann so konfiguriert werden, dass eine E-Mail-Nachricht nach einer konfigurierbaren Anzahl von Anmeldefehlern innerhalb eines definierbaren Zeitraums gesendet wird. Die Anzahl der Anmeldefehler kann zwischen 3 und 7 betragen und der Zeitraum zwischen 5 Minuten und 24 Stunden.

Der Computer, auf dem die Software installiert ist, muss mit einem SMTP-Server mit offenem Port kommunizieren können.

1. Öffnen Sie den Arbeitsbereich „Konfiguration“.
2. Klicken Sie auf **Benutzerverwaltung**.
3. Öffnen Sie die Registerkarte Sicherheitsmodus.
4. Aktivieren Sie das Kontrollkästchen **E-Mail-Nachrichten senden nach** und geben Sie dann an, wie viele Anmeldefehler innerhalb welchen Zeitraums (in Minuten) eine E-Mail-Benachrichtigung generieren sollen.

   Tipp! Um die Benachrichtigung zu deaktivieren, deaktivieren Sie das Kontrollkästchen **E-Mail-Nachrichten senden nach**.
5. Im Feld **SMTP-Server** geben Sie den Namen des SMTP-Servers ein.

   Hinweis: Das SMTP-Konto sendet Mails an den E-Mail-Server. Der SMTP-Server ist in der E-Mail-Anwendung des Unternehmens definiert.
6. Geben Sie im Feld **Portnummer** die Nummer des offenen Ports ein.
   Klicken Sie auf **Standard anwenden**, um die Standard-Port-Nummer 25 einzufügen.
7. Geben Sie im Feld **Bis** die E-Mail-Adresse ein, an die die Nachricht gesendet werden soll. Beispiel: username@domain.com.
8. Geben Sie im Feld **Von** die E-Mail-Adresse ein, die im Feld **Von** der Nachricht angezeigt werden soll.
9. Im Feld **Betreff** geben Sie den Betreff der Nachricht ein.
10. Geben Sie im Feld **Nachricht** den Text ein, der im Nachrichtentext enthalten sein soll.
11. Klicken Sie auf **Speichern**.

Ein Bestätigungsdialogfeld wird geöffnet.

12. Klicken Sie auf **OK**.
13. Um die Konfiguration zu überprüfen, klicken Sie auf **Test-Mail senden**.

Konfiguration des Zugriffs auf die SCIEX OS Software

Gehen Sie folgendermaßen vor, bevor Sie die Sicherheit konfigurieren:

- Entfernen Sie alle unnötigen Benutzer und Benutzergruppen, wie z. B. „Replicator“, „Power User“ und „Backup Operator“, vom lokalen Computer und vom Netzwerk.

  Hinweis: Jeder SCIEX Computer ist mit einem lokalen Konto auf Administratorebene, **abservice**, konfiguriert. Dieses Konto wird vom SCIEX-Kundendienst und dem technischen Support für das Installieren, Warten und Unterstützen des Systems verwendet. Dieses Konto darf nicht gelöscht oder deaktiviert werden. Wenn das Konto gelöscht oder deaktiviert werden muss, dann entwickeln Sie einen alternativen Plan für den SCIEX-Zugriff und teilen Sie dies dem zuständigen Außendienstmitarbeiter mit.

- Fügen Sie Benutzergruppen hinzu, die Gruppen ohne administrative Aufgaben enthalten.
- Konfigurieren Sie die Systemberechtigungen.
- Erstellen Sie anhand von Gruppenrichtlinien geeignete Verfahren und Kontenrichtlinien für die Benutzer.

In der Windows-Dokumentation finden Sie weitere Informationen zu folgenden Themen:

- Benutzer und Gruppen und Active-Directory-Benutzer
- Passwort und Kontosperrrichtlinien für Benutzerkonten
- Richtlinien zu Benutzerrechten

Wenn Benutzer in einer „Active Directory“-Umgebung arbeiten, wirken sich die Einstellungen der „Active Directory“-Gruppenrichtlinien auf die Computer-Sicherheit aus. Besprechen Sie im Rahmen einer umfassenden Bereitstellung der SCIEX OS-Software die Gruppenrichtlinien mit dem Active-Directory-Administrator.

SCIEX OS Berechtigungen

Abbildung 4-1: Seite „User Management“

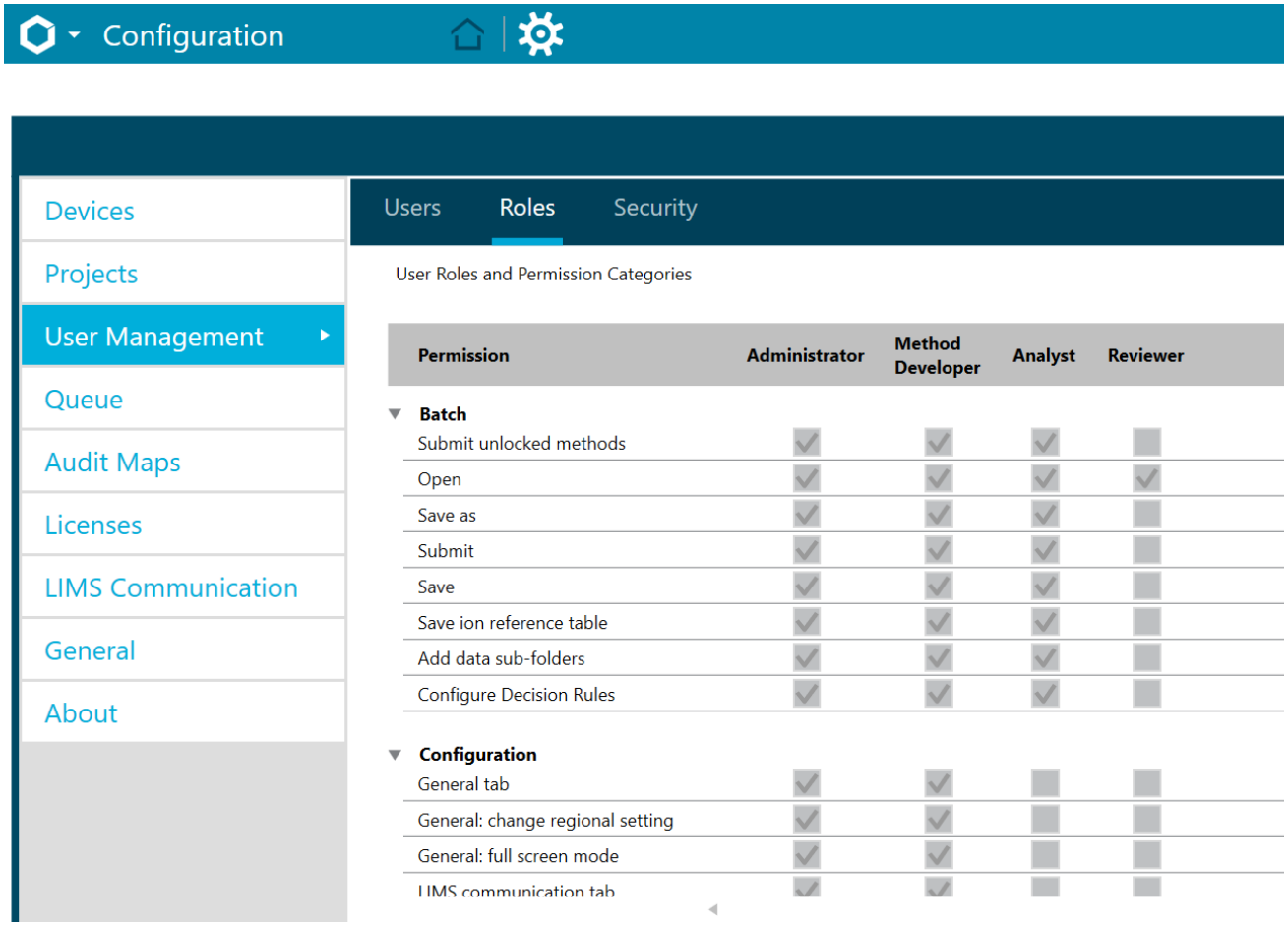


Tabelle 4-3: Berechtigungen

Berechtigung	Beschreibung
Batch	
Entsperrte Methoden zur Warteliste senden	Erlaubt den Benutzern das Übergeben von Batches, die entsperrte Methoden enthalten.
Öffnen	Erlaubt den Benutzern das Öffnen bestehender Batches.
Speichern unter	Erlaubt den Benutzern das Speichern von Batches unter einem neuen Namen.
Zur Warteliste senden	Erlaubt den Benutzern das Übergeben von Batches.
Speichern	Erlaubt den Benutzern das Speichern eines Batches und das Überschreiben der vorhandenen Inhalte.
Ionenreferenztabelle speichern	Erlaubt den Benutzern die Bearbeitung der Ionenreferenztabelle.

Tabelle 4-3: Berechtigungen (Fortsetzung)

Berechtigung	Beschreibung
Daten-Unterordner hinzufügen	Erlaubt den Benutzern das Erstellen von Unterordnern für das Speichern von Daten.
Entscheidungsregeln konfigurieren	Erlaubt den Benutzern das Hinzufügen und Ändern von Entscheidungsregeln.
Konfiguration	
Registerkarte „Allgemein“	Erlaubt den Benutzern das Öffnen der Seite „Allgemein“ im Arbeitsbereich „Konfiguration“.
Allgemein: Regionseinstellungen ändern	Erlaubt den Benutzern das Anwenden der regionalen Einstellungen des aktiven Systems auf die SCIEX OS Software.
Allgemein: Vollbildmodus	Erlaubt den Benutzern die Aktivierung bzw. Deaktivierung des Vollbildmodus.
Allgemein: Windows-Dienste stoppen	Erlaubt es den Benutzern die Option **Windows-Einstellungen** zu aktivieren oder zu deaktivieren.
Registerkarte „LIMS-Kommunikation“	Erlaubt den Benutzern das Öffnen der Seite „LIMS-Kommunikation“ im Arbeitsbereich „Konfiguration“.
Registerkarte „Audit-Maps“	Erlaubt den Benutzern das Öffnen der Seite „Audit-Maps“ im Arbeitsbereich „Konfiguration“.
Registerkarte „Warteschlange“	Erlaubt den Benutzern das Öffnen der Seite „Warteschlange“ im Arbeitsbereich „Konfiguration“.
Warteschlange: Geräteleerlaufzeit	Erlaubt den Benutzern die Einstellung der Geräteleerlaufzeit.
Warteschlange: Maximale Anzahl erfasster Proben	Erlaubt den Benutzern die Einstellung der maximal zulässigen Anzahl an erfassten Proben.
Warteschlange: Andere Warteschlangeneinstellungen	Erlaubt den Benutzern die Konfiguration anderer Warteschlangeneinstellungen.
Registerkarte „Projekte“	Erlaubt den Benutzern das Öffnen der Seite „Projekte“ im Arbeitsbereich „Konfiguration“.
Projekte: Projekt erstellen	Erlaubt den Benutzern das Erstellen von Projekten.
Projekte: Eine Audit-Map-Vorlage auf ein bestehendes Projekt anwenden	Erlaubt den Benutzern die Anwendung einer Audit-Map auf ein Projekt.
Projekte: Stammverzeichnis erstellen	Erlaubt den Benutzern das Erstellen eines Stammverzeichnisses für das Speichern von Projekten.

Tabelle 4-3: Berechtigungen (Fortsetzung)

Berechtigung	Beschreibung
Projekte: Aktuelles Stammverzeichnis festlegen	Erlaubt den Benutzern das Ändern des Stammverzeichnisses für ein Projekt.
Projekte: Netzwerkanmeldedaten festlegen	Erlaubt den Benutzern das Festlegen eines sicheren Netzwerkkontos (SNA), das während der Netzwerkerfassung verwendet wird, wenn der angemeldete Benutzer keinen Zugriff auf die Netzwerkressource hat.
Projekte: Das Schreiben der Prüfsumme für die wiff-Datenerstellung aktivieren	Erlaubt den Benutzern das Konfigurieren der Software, um Prüfsummen in `wiff`-Datendateien zu schreiben.
Projekte: Stammverzeichnis löschen	Benutzer können ein Stammverzeichnis aus der Liste löschen.
Registerkarte „Geräte“	Erlaubt den Benutzern das Öffnen der Seite „Geräte“ im Arbeitsbereich „Konfiguration“.
Registerkarte „Benutzerverwaltung“	Erlaubt den Benutzern das Öffnen der Seite „Benutzerverwaltung“ im Arbeitsbereich „Konfiguration“.
Abmeldung des Benutzers erzwingen	Erlaubt den Benutzern, die Abmeldung eines bei der SCIEX OS Software angemeldeten Benutzers zu erzwingen.
Registerkarte „CAC“ [1]	Erlaubt den Benutzern das Öffnen der Seite „CAC“ im Arbeitsbereich „Konfiguration“.
Registerkarte „Druckvorlagen“	Erlaubt Benutzern, die Registerkarte „Druckvorlagen“ im Arbeitsbereich „Konfiguration“ zu öffnen.
Druckvorlagen: Druckvorlagen erstellen und modifizieren	Erlaubt Benutzern, neue Druckvorlagen zu erstellen oder bestehende Druckvorlagen zu ändern.
Druckvorlagen: Standard-Druckvorlage festlegen	Erlaubt Benutzern, die aktive Druckvorlage als Standard für das aktive Projekt festzulegen.
Druckvorlagen: Die aktuelle Vorlage auf alle Projekte im Stammverzeichnis anwenden	Erlaubt Benutzern, die Druckvorlage zur Liste der verfügbaren Druckvorlagen für ausgewählte Projekte in einem ausgewählten Stammverzeichnis hinzuzufügen.
Ereignisprotokoll	

[1] In Version 3.1 wurde die Berechtigung **Zentraladministration aktivieren** umbenannt in **CAC**. Die Seite CAC im Arbeitsbereich „Konfiguration“ kann verwendet werden, um die Zentraladministration der SCIEX OS Software zu konfigurieren.

Tabelle 4-3: Berechtigungen (Fortsetzung)

Berechtigung	Beschreibung
Auf Arbeitsbereich „Ereignisprotokoll“ zugreifen	Erlaubt den Benutzern das Öffnen des Arbeitsbereichs „Ereignisprotokoll“.
Protokoll archivieren	Erlaubt Benutzern, die Protokolle im Arbeitsbereich „Ereignisprotokoll“ zu archivieren.
Audit-Trail	
Auf Arbeitsbereich „Audit-Trail“ zugreifen	Erlaubt den Benutzern das Öffnen des Arbeitsbereichs „Audit-Trail“.
Aktive Audit-Map anzeigen	Erlaubt den Benutzern das Anzeigen der aktiven Audit-Map für eine Workstation oder ein Projekt im Arbeitsbereich „Audit Trail“.
Audit-Trail drucken/ exportieren	Erlaubt den Benutzern das Drucken oder Exportieren des Audit-Trails.
Feld „Datenerfassung“	
Start	Erlaubt den Benutzern das Starten der Erfassung im Teilfenster „Datenerfassung“.
Stopp	Erlaubt den Benutzern das Stoppen der Erfassung im Teilfenster „Datenerfassung“.
Speichern	Erlaubt den Benutzern das Speichern von erfassten Daten mit einem anderen Dateinamen im Teilfenster „Datenerfassung“.
MS- und LC-Methode	
Auf Arbeitsbereich „Methode“ zugreifen	Erlaubt den Benutzern das Öffnen der Arbeitsbereiche „MS-Methode“ und „LC-Methode“.
Neu	Erlaubt den Benutzern die Erstellung von MS- und LC-Methoden.
Öffnen	Erlaubt den Benutzern das Öffnen von MS- und LC-Methoden.
Speichern	Erlaubt den Benutzern das Speichern einer Methode und das Überschreiben der vorhandenen Inhalte.
Speichern unter	Erlaubt den Benutzern das Speichern von Methoden unter einem neuen Namen.
Methode sperren/ entsperren	Erlaubt den Benutzern das Sperren von Methoden, um deren Bearbeitung zu verhindern, sowie das Entsperren von Methoden.
Warteschlange	

Tabelle 4-3: Berechtigungen (Fortsetzung)

Berechtigung	Beschreibung
Verwalten	Erlaubt den Benutzern das Öffnen des Arbeitsbereichs „Warteschlange“.
Start/Stopp	Erlaubt den Benutzern das Starten und Stoppen der Warteschlange.
Drucken	Erlaubt den Benutzern das Drucken der Warteschlange.
Probe bearbeiten	Erlaubt den Benutzern das Ändern des Namens oder der Datendatei einer Probe.
Bibliothek	
Auf Arbeitsbereich „Bibliothek“ zugreifen	Erlaubt den Benutzern das Öffnen des Arbeitsbereichs „Bibliothek“. Gilt nicht für den Quantifizierungs-Arbeitsablauf.
MS Tune	
Auf Arbeitsbereich „MS Tune“ zugreifen	Erlaubt den Benutzern das Öffnen des Arbeitsbereichs „MS Tune“.
Erweitertes MS-Tuning	X500 QTOF- und ZenoTOF 7600-Systeme: Erlaubt den Benutzern den Zugriff auf erweiterte Tuning-Optionen, einschließlich **Optimieren des Detektors**, **Positive TOF-Abstimmung**, **Negative TOF-Abstimmung**, **Positive Q1-Einheitenabstimmung**, **Negative Q1-Einheitenabstimmung**, **Positive Q1-Hoch-Abstimmung** und **Negative Q1-Hoch-Abstimmung**.
Erweiterte Fehlerbehebung	Erlaubt den Benutzern das Öffnen des Dialogfeldes „Erweiterte Fehlerbehebung“.
Schnelle Statusüberprüfung	X500 QTOF- und ZenoTOF 7600-Systeme: Erlaubt den Benutzern das Ausführen des **Positive schnelle Statusüberprüfung** und **Negative schnelle Statusüberprüfung**.
Instrumentendaten wiederherstellen	Erlaubt den Benutzern die Wiederherstellung zuvor gespeicherter Tuning-Einstellungen.
Explorer	
Auf Arbeitsbereich „Explorer“ zugreifen	Erlaubt den Benutzern das Öffnen des Arbeitsbereichs „Explorer“.
Exportieren	Erlaubt den Benutzern das Exportieren von Daten aus dem Arbeitsbereich „Explorer“.
Drucken	Erlaubt den Benutzern das Drucken von Daten im Arbeitsbereich „Explorer“.
Optionen	Erlaubt den Benutzern das Ändern der Optionen für den Arbeitsbereich „Explorer“.

Tabelle 4-3: Berechtigungen (Fortsetzung)

Berechtigung	Beschreibung
Erneut kalibrieren	Erlaubt den Benutzern das erneute Kalibrieren von Proben und Spektren im Arbeitsbereich „Explorer“. Gilt nicht für den Quantifizierungs-Arbeitsablauf.
Analyse	
Neue Ergebnisse	Erlaubt den Benutzern die Erstellung von Ergebnistabellen.
Prozessierungsmethode erstellen	Erlaubt den Benutzern die Erstellung von Prozessierungsmethoden.
Prozessierungsmethode ändern	Erlaubt den Benutzern das Ändern von Prozessierungsmethoden.
Export nicht gesperrter Ergebnistabelle und Erstellen eines Berichts aus dieser erlauben	Erlaubt den Benutzern, eine nicht gesperrte Ergebnistabelle oder Statistiktabelle zu exportieren und einen Bericht aus dieser zu erstellen.
Ergebnisse speichern für Automatisierungs-Batch	Ermöglicht das Speichern von Ergebnistabellen, die im Arbeitsbereich „Batch“ automatisch erstellt wurden. Diese Berechtigung ist für die automatische Prozessierung während der Erfassung erforderlich.
Integrationsalgorithmus der standardmäßigen Quantifizierungsmethode ändern	Erlaubt den Benutzern das Ändern des Integrationsalgorithmus in den Standardeinstellungen des Projekts.
Integrationsparameter der standardmäßigen Quantifizierungsmethode ändern	Erlaubt den Benutzern das Ändern der Integrationsparameter in den Standardeinstellungen des Projekts.
Warnung bei geänderten Peaks eines Projekts aktivieren	Erlaubt den Benutzern die Freigabe von Warnungen bei geänderten Peaks für ein Projekt.
Proben hinzufügen	Erlaubt den Benutzern das Hinzufügen von Proben zu einer Ergebnistabelle.
Ausgewählte Proben entfernen	Erlaubt den Benutzern das Entfernen von Proben aus einer Ergebnistabelle.
Externe Kalibrierung exportieren, importieren oder entfernen	Erlaubt den Benutzern das Exportieren, Importieren oder Entfernen externer Kalibrierungen.
Probenname ändern	Erlaubt den Benutzern das Ändern des Probennamens in der Ergebnistabelle.

Tabelle 4-3: Berechtigungen (Fortsetzung)

Berechtigung	Beschreibung
Probentyp ändern	Erlaubt den Benutzern das Ändern des Probentyps in der Ergebnistabelle. Gültige Probentypen umfassen Standard, Qualitätskontrolle (QC) und Unbekannt.
Proben-ID ändern	Erlaubt den Benutzern das Ändern der Proben-ID in der Ergebnistabelle.
Ist-Konzentration ändern	Erlaubt den Benutzern das Ändern der Ist-Konzentration der Standard- und QC-Proben in der Ergebnistabelle.
Verdünnungsfaktor ändern	Erlaubt den Benutzern das Ändern des Verdünnungsfaktors in der Ergebnistabelle.
Kommentarfelder ändern	Erlaubt den Benutzern das Ändern der folgenden Kommentarfelder: • **Komponentenkommentar** • **IS Kommentar** • **IS Peak-Kommentar** • **Peak-Kommentar** • **Probenkommentar**
Manuelle Integration aktivieren	Erlaubt den Benutzern die Durchführung einer manuellen Integration.
Peak auf „nicht gefunden“ setzen	Erlaubt den Benutzern das Setzen eines Peaks auf **Nicht gefunden**.
Einen Peak in die Ergebnistabelle einbeziehen oder aus dieser ausschließen	Erlaubt den Benutzern das Einschließen von Peaks in die Ergebnistabelle und das Ausschließen aus dieser.
Regressionsoptionen	Erlaubt den Benutzern das Ändern der Regressionsoptionen im Bereich „Kalibrierkurve“.
Integrationsparameter der Ergebnistabelle für ein einzelnes Chromatogramm ändern	Erlaubt den Benutzern das Ändern der Integrationsparameter für ein Einzelchromatogramm im Bereich „Peak Review“.
Quantifizierungsmethode für Komponente der Ergebnistabelle modifizieren	Erlaubt den Benutzern die Auswahl einer anderen Prozessierungsmethode für eine Komponente im Bereich „Peak Review“ mit der Option **Prozessierungsmethode für Komponente aktualisieren**.
Neue Einstellungen für metrische Darstellungen erstellen	Erlaubt den Benutzern die Erstellung neuer metrischer Darstellungen sowie die Änderung der Einstellungen.

Tabelle 4-3: Berechtigungen (Fortsetzung)

Berechtigung	Beschreibung
Benutzerdefinierte Spalten hinzufügen	Erlaubt den Benutzern das Hinzufügen von benutzerdefinierten Spalten zu einer Ergebnistabelle.
Titelformat für die Peak-Überprüfung festlegen	Erlaubt den Benutzern das Ändern des Titels der Peaküberprüfung.
Benutzerdefinierte Spalte entfernen	Erlaubt den Benutzern das Entfernen von benutzerdefinierten Spalten aus einer Ergebnistabelle.
Einstellungen für die Anzeige der Ergebnistabelle	Erlaubt den Benutzern die benutzerdefinierte Anpassung der Spalten, die in der Ergebnistabelle angezeigt werden.
Ergebnistabelle sperren	Erlaubt den Benutzern das Sperren einer Ergebnistabelle, um deren Bearbeitung zu verhindern.
Ergebnistabelle entsperren	Erlaubt den Benutzern das Entsperren einer Ergebnistabelle, um Änderungen vorzunehmen.
Ergebnisdatei als „geprüft“ kennzeichnen und speichern	Erlaubt den Benutzern die Kennzeichnung einer Ergebnistabelle als „geprüft“ sowie deren Speicherung.
Berichtsvorlage ändern	Erlaubt den Benutzern das Ändern von Berichtsvorlagen.
Ergebnisse an LIMS übertragen	Erlaubt den Benutzer den Upload von Ergebnissen in ein Laboratory Information Management System (LIMS).
Barcode-Spalte ändern	Erlaubt den Benutzern das Ändern der Spalte **Barcode** in einer Ergebnistabelle.
Zuweisung der Vergleichsprobe ändern	Erlaubt den Benutzern das Ändern der Vergleichsprobe, die in der Spalte **Vergleich** der Ergebnistabelle angegeben ist.
MSMS-Spektren zur Bibliothek hinzufügen	Erlaubt den Benutzern das Hinzufügen der ausgewählten MS/MS-Spektren zu einer Bibliothek. Gilt nicht für den Quantifizierungs-Arbeitsablauf.
Standardeinstellungen des Projekts	Erlaubt den Benutzern das Ändern der Standardeinstellungen des Projekts für die quantitative und qualitative Prozessierung.
Bericht in allen Formaten erstellen	Erlaubt den Benutzern, Berichte in allen Formaten zu erstellen. Benutzer ohne Berechtigung können Berichte nur im PDF-Format generieren.
Parameter für die Markierungskriterien bearbeiten	Erlaubt den Benutzern das Ändern der Parameter für die Markierung in einer Prozessierungsmethode.

Tabelle 4-3: Berechtigungen (Fortsetzung)

Berechtigung	Beschreibung
Parameter für das automatische Entfernen von Ausreißern ändern	Erlaubt den Benutzern das Ändern der Parameter für das automatische Entfernen von Ausreißern.
Automatische Entfernung von Ausreißern aktivieren	Erlaubt den Benutzern das Ändern der Prozessierungsmethode, um das automatische Entfernen von Ausreißern zu aktivieren.
Prozessierungsmethode über FF/LS aktualisieren	Erlaubt den Benutzern das Verwenden der Formelsuche und Bibliothekssuche zum Aktualisieren von Prozessierungsmethoden. Gilt nicht für den Quantifizierungs-Arbeitsablauf.
Ergebnisse über FF/LS aktualisieren	Erlaubt den Benutzern das Verwenden der Formelsuche und Bibliothekssuche zum Aktualisieren der Ergebnisse. Gilt nicht für den Quantifizierungs-Arbeitsablauf.
Funktion der Gruppierung nach Addukten aktivieren	Erlaubt den Benutzern die Aktualisierung der Prozessierungsmethode, um die Funktion zur Gruppierung von Addukten zu verwenden.
Dateien suchen	Erlaubt den Benutzern das Suchen außerhalb des lokalen Datenordners.
Standardzugabe aktivieren	Erlaubt den Benutzern die Aktualisierung der Prozessierungsmethode, um die Funktion „Standard Addition“ zu aktivieren.
Prozentsatzregel für die manuelle Integration festlegen	Erlaubt den Benutzern die Änderung des Parameters **Manuelle Integration %**.
Gewicht/Volumen ändern	Ermöglicht den Benutzern das Ändern des Feldes **Gewicht/ Volumen**.

Über Benutzer und Rollen

In der SCIEX OS Software kann der Administrator Windows-Benutzer und -Gruppen zur Datenbank für die Benutzerverwaltung hinzufügen. Für den Zugriff auf die Software müssen Benutzer in der Datenbank für die Benutzerverwaltung sein oder sie müssen ein Mitglied einer der Gruppen in der Datenbank sein.

Benutzer können einer oder mehreren voreingestellten Rollen, die in der folgenden Tabelle angezeigt werden, oder auch benutzerdefinierten Rollen, zugewiesen werden, falls dies erforderlich ist. Die Funktionen, auf die ein Benutzer zugreifen kann, werden durch Rollen angegeben. Die voreingestellten Rollen können nicht gelöscht und ihre Berechtigungen nicht geändert werden.

Hinweis: Für Arbeitsgruppen, die mit der Central Administrator Console (CAC) Software verwaltet werden, sind die Seiten „Benutzerverwaltung“ schreibgeschützt.

Tabelle 4-4: Voreingestellte Rollen

Rolle	Typische Aufgaben
Administrator	• Verwaltet das System • Konfiguriert die Sicherheit
Methodenentwickler	• Erstellt Methoden • Führt Batches aus • Analysiert Daten zur Verwendung durch den Benutzer
Analyst	• Führt Batches aus • Analysiert Daten zur Verwendung durch den Benutzer
Prüfer	• Prüft Daten • Prüft Audit-Trails • Bewertet Quantifizierungsergebnisse

Tabelle 4-5: Voreingestellte Berechtigungen

Berechtigung	Administrator	Methodenentwickler	Analyst	Prüfer
Batch				
Entsperrte Methoden zur Warteliste senden	✓	✓	✓	×
Öffnen	✓	✓	✓	✓
Speichern unter	✓	✓	✓	×
Zur Warteliste senden	✓	✓	✓	×
Speichern	✓	✓	✓	×
Ionenreferenztabelle speichern	✓	✓	✓	×
Daten-Unterordner hinzufügen	✓	✓	✓	×
Entscheidungsregeln konfigurieren	✓	✓	✓	×
Konfiguration				

Tabelle 4-5: Voreingestellte Berechtigungen (Fortsetzung)

Berechtigung	Administrator	Methodenentwickler	Analyst	Prüfer
Registerkarte „Allgemein“	✓	✓	×	×
Allgemein: Regionseinstellungen ändern	✓	✓	×	×
Allgemein: Vollbildmodus	✓	✓	×	×
Allgemein: Windows-Dienste stoppen	✓	×	×	×
Registerkarte „LIMS-Kommunikation“	✓	✓	×	×
Registerkarte „Audit-Maps“	✓	×	×	×
Registerkarte „Warteschlange“	✓	✓	✓	✓
Warteschlange: Geräteleerlaufzeit	✓	✓	×	×
Warteschlange: Maximale Anzahl erfasster Proben	✓	✓	×	×
Warteschlange: Andere Warteschlangeneinstellungen	✓	✓	×	×
Registerkarte „Projekte“	✓	✓	✓	✓
Projekte: Projekt erstellen	✓	✓	✓	×
Projekte: Eine Audit-Map-Vorlage auf ein bestehendes Projekt anwenden	✓	×	×	×
Projekte: Stammverzeichnis erstellen	✓	×	×	×

Tabelle 4-5: Voreingestellte Berechtigungen (Fortsetzung)

Berechtigung	Administrator	Methodenentwickler	Analyst	Prüfer
Projekte: Aktuelles Stammverzeichnis festlegen	✓	×	×	×
Projekte: Netzwerkanmeldedaten festlegen	✓	×	×	×
Projekte: Das Schreiben der Prüfsumme für die wiff-Datenerstellung aktivieren	✓	×	×	×
Projekte: Stammverzeichnis löschen	✓	×	×	×
Registerkarte „Geräte“	✓	✓	✓	×
Registerkarte „Benutzerverwaltung“	✓	×	×	×
Abmeldung des Benutzers erzwingen	✓	×	×	×
Registerkarte „CAC“[1]	✓	×	×	×
Registerkarte „Druckvorlagen“	✓	✓	×	×
Druckvorlagen: Druckvorlagen erstellen und modifizieren	✓	✓	×	×
Druckvorlagen: Standard-Druckvorlage festlegen	✓	✓	×	×

[1] In Version 3.1 wurde die Berechtigung **Zentraladministration aktivieren** umbenannt in **CAC**. Die Seite CAC im Arbeitsbereich „Konfiguration“ kann verwendet werden, um die Zentraladministration der SCIEX OS Software zu konfigurieren.

Tabelle 4-5: Voreingestellte Berechtigungen (Fortsetzung)

Berechtigung	Administrator	Methodenentwickler	Analyst	Prüfer
Druckvorlagen: Die aktuelle Vorlage auf alle Projekte im Stammverzeichnis anwenden	✓	×	×	×
Ereignisprotokoll				
Auf Arbeitsbereich „Ereignisprotokoll“ zugreifen	✓	✓	✓	✓
Protokoll archivieren	✓	✓	✓	✓
Audit-Trail				
Auf Arbeitsbereich „Audit-Trail“ zugreifen	✓	✓	✓	✓
Aktive Audit-Map anzeigen	✓	✓	✓	✓
Audit-Trail drucken/ exportieren	✓	✓	✓	✓
Feld „Datenerfassung“				
Start	✓	✓	✓	×
Stopp	✓	✓	✓	×
Speichern	✓	✓	✓	×
MS- und LC-Methode				
Auf Arbeitsbereich „Methode“ zugreifen	✓	✓	✓	✓
Neu	✓	✓	×	×
Öffnen	✓	✓	✓	✓
Speichern	✓	✓	×	×
Speichern unter	✓	✓	×	×
Methode sperren/ entsperren	✓	✓	×	×
Warteschlange				
Verwalten	✓	✓	✓	×

Tabelle 4-5: Voreingestellte Berechtigungen (Fortsetzung)

Berechtigung	Administrator	Methodenentwickler	Analyst	Prüfer
Start/Stopp	✓	✓	✓	×
Drucken	✓	✓	✓	✓
Probe bearbeiten	✓	✓	×	×
Bibliothek				
Auf Arbeitsbereich „Bibliothek“ zugreifen	✓	✓	✓	✓
MS Tune				
Auf Arbeitsbereich „MS Tune“ zugreifen	✓	✓	✓	×
Erweitertes MS-Tuning	✓	✓	×	×
Erweiterte Fehlerbehebung	✓	✓	×	×
Schnelle Statusüberprüfung	✓	✓	✓	×
Instrumentendaten wiederherstellen	✓	✓	×	×
Explorer				
Auf Arbeitsbereich „Explorer“ zugreifen	✓	✓	✓	✓
Exportieren	✓	✓	✓	×
Drucken	✓	✓	✓	×
Optionen	✓	✓	✓	×
Erneut kalibrieren	✓	✓	×	×
Analyse				
Neue Ergebnisse	✓	✓	✓	×
Prozessierungsmethode erstellen	✓	✓	✓	×
Prozessierungsmethode ändern	✓	✓	×	×

Tabelle 4-5: Voreingestellte Berechtigungen (Fortsetzung)

Berechtigung	Administrator	Methodenentwickler	Analyst	Prüfer
Export nicht gesperrter Ergebnistabelle und Erstellen eines Berichts aus dieser erlauben	✓	×	×	×
Ergebnisse speichern für Automatisierungs-Batch	✓	✓	✓	×
Integrationsalgorithmus der standardmäßigen Quantifizierungsmethode ändern	✓	✓	×	×
Integrationsparameter der standardmäßigen Quantifizierungsmethode ändern	✓	✓	×	×
Warnung bei geänderten Peaks eines Projekts aktivieren	✓	×	×	×
Proben hinzufügen	✓	✓	✓	×
Ausgewählte Proben entfernen	✓	✓	✓	×
Externe Kalibrierung exportieren, importieren oder entfernen	✓	✓	✓	×
Probenname ändern	✓	✓	✓	×
Probentyp ändern	✓	✓	✓	×
Proben-ID ändern	✓	✓	✓	×
Ist-Konzentration ändern	✓	✓	✓	×
Verdünnungsfaktor ändern	✓	✓	✓	×

Tabelle 4-5: Voreingestellte Berechtigungen (Fortsetzung)

Berechtigung	Administrator	Methodenentwickler	Analyst	Prüfer
Kommentarfelder ändern	✓	✓	✓	×
Manuelle Integration aktivieren	✓	✓	✓	×
Peak auf „nicht gefunden“ setzen	✓	✓	✓	×
Einen Peak in die Ergebnistabelle einbeziehen oder aus dieser ausschließen	✓	✓	✓	×
Regressionsoptionen	✓	✓	✓	×
Integrationsparameter der Ergebnistabelle für ein einzelnes Chromatogramm ändern	✓	✓	✓	×
Quantifizierungsmethode für Komponente der Ergebnistabelle modifizieren	✓	✓	✓	×
Neue Einstellungen für metrische Darstellungen erstellen	✓	✓	✓	✓
Benutzerdefinierte Spalten hinzufügen	✓	✓	✓	×
Titelformat für die Peak-Überprüfung festlegen	✓	×	×	×
Benutzerdefinierte Spalte entfernen	✓	✓	×	×
Einstellungen für die Anzeige der Ergebnistabelle	✓	✓	✓	✓
Ergebnistabelle sperren	✓	✓	✓	✓

Tabelle 4-5: Voreingestellte Berechtigungen (Fortsetzung)

Berechtigung	Administrator	Methodenentwickler	Analyst	Prüfer
Ergebnistabelle entsperren	✓	×	×	×
Ergebnisdatei als „geprüft“ kennzeichnen und speichern	✓	×	×	✓
Berichtsvorlage ändern	✓	✓	×	×
Ergebnisse an LIMS übertragen	✓	✓	✓	×
Barcode-Spalte ändern	✓	✓	×	×
Zuweisung der Vergleichsprobe ändern	✓	✓	×	×
MSMS-Spektren zur Bibliothek hinzufügen	✓	✓	×	×
Standardeinstellungen des Projekts	✓	✓	×	×
Bericht in allen Formaten erstellen	✓	✓	✓	✓
Parameter für die Markierungskriterien bearbeiten	✓	✓	✓	×
Parameter für das automatische Entfernen von Ausreißern ändern	✓	✓	×	×
Automatische Entfernung von Ausreißern aktivieren	✓	✓	✓	×
Prozessierungsmethode über FF/LS aktualisieren	✓	✓	×	×
Ergebnisse über FF/LS aktualisieren	✓	✓	×	×

Tabelle 4-5: Voreingestellte Berechtigungen (Fortsetzung)

Berechtigung	Administrator	Methodenentwickler	Analyst	Prüfer
Funktion der Gruppierung nach Addukten aktivieren	✓	✓	×	×
Dateien suchen	✓	✓	✓	✓
Standardzugabe aktivieren	✓	✓	✓	×
Prozentsatzregel für die manuelle Integration festlegen	✓	×	×	×
Gewicht/Volumen ändern	✓	✓	✓	×

Verwalten von Benutzern

Hinzufügen eines Benutzers oder einer Gruppe

1. Öffnen Sie den Arbeitsbereich „Konfiguration“.
2. Öffnen Sie die Seite „Benutzerverwaltung“.
3. Öffnen Sie die Registerkarte „Benutzer“.
4. Klicken Sie auf **Benutzer hinzufügen** ( ).
   Das Dialogfeld „Benutzer oder Gruppe auswählen“ wird geöffnet.
5. Geben Sie den Namen des Benutzers oder der Gruppe ein und klicken Sie dann auf **OK**.

   Tipp! Für Informationen über das Dialogfeld „Benutzer oder Gruppe auswählen“ und seine Verwendung, klicken Sie auf **F1**.
6. Um den Benutzer zu aktivieren, stellen Sie sicher, dass das Kontrollkästchen **Aktive(r) Benutzer oder Gruppe** ausgewählt ist.
7. Wählen Sie im Bereich **Rollen** eine oder mehrere Rollen aus und klicken Sie dann auf **Speichern**.

Deaktivieren von Benutzern oder Gruppen

1. Öffnen Sie den Arbeitsbereich „Konfiguration“.
2. Öffnen Sie die Seite „Benutzerverwaltung“.
3. Öffnen Sie die Registerkarte „Benutzer“.
4. Wählen Sie aus der Liste **Benutzername oder Gruppe** den zu deaktivierenden Benutzer oder die zu deaktivierende Gruppe aus.

5. Deaktivieren Sie das Kontrollkästchen **Aktive(r) Benutzer oder Gruppe**.
   Die Software fordert Sie zur Bestätigung auf.
6. Klicken Sie auf **Ja**.

Entfernen von Benutzern oder Gruppen

Gehen Sie nach diesem Verfahren vor, um einen Benutzer oder eine Gruppe aus der Software zu entfernen. Wird ein Benutzer oder eine Gruppe aus Windows entfernt, muss er auch aus der SCIEX OS Software entfernt werden.

1. Öffnen Sie den Arbeitsbereich „Konfiguration“.
2. Öffnen Sie die Seite „Benutzerverwaltung“.
3. Öffnen Sie die Registerkarte „Benutzer“.
4. Wählen Sie aus der Liste **Benutzername oder Gruppe** den zu entfernenden Benutzer oder die zu entfernende Gruppe aus.
5. Klicken Sie auf **Löschen**.
   Die Software fordert Sie zur Bestätigung auf.
6. Klicken Sie auf **OK**.

Verwalten von Rollen

Ändern der einem Benutzer oder einer Gruppe zugewiesenen Rolle

Mit diesem Verfahren können Sie einem Benutzer oder einer Gruppe neue Rollen zuweisen oder vorhandene Rollenzuweisungen entfernen.

1. Öffnen Sie den Arbeitsbereich „Konfiguration“.
2. Öffnen Sie die Seite „Benutzerverwaltung“.
3. Öffnen Sie die Registerkarte „Benutzer“.
4. Wählen Sie im Feld **Benutzername oder Gruppe** den zu ändernden Benutzer oder die zu ändernde Gruppe aus.
5. Wählen Sie die dem Benutzer oder der Gruppe zuzuweisenden Rollen aus und löschen Sie alle zu entfernenden Rollen.
6. Klicken Sie auf **Speichern**.

Erstellen einer benutzerdefinierten Rolle

1. Öffnen Sie den Arbeitsbereich „Konfiguration“.
2. Öffnen Sie die Seite „Benutzerverwaltung“.
3. Öffnen Sie die Registerkarte „Rollen“.
4. Klicken Sie auf **Rolle hinzufügen** ().
   Das Dialogfeld Benutzerrolle duplizieren wird geöffnet.

5. Wählen Sie im Feld **Vorhandene Benutzerrolle** die Rolle aus, die als Vorlage für die neue Rolle verwendet werden soll.
6. Geben Sie einen Namen und eine Beschreibung für die Rolle ein und klicken Sie dann auf **OK**.
7. Wählen Sie die Zugriffsberechtigungen für die Rolle aus.
8. Klicken Sie auf **Alle Rollen speichern**.
9. Klicken Sie auf **OK**.

Löschen einer benutzerdefinierten Rolle

Hinweis: Wenn ein Benutzer nur der zu löschenden Rolle zugewiesen ist, fordert das System zum Löschen des Benutzers sowie der Rolle auf.

1. Öffnen Sie den Arbeitsbereich „Konfiguration“.
2. Öffnen Sie die Seite „Benutzerverwaltung“.
3. Öffnen Sie die Registerkarte „Rollen“.
4. Klicken Sie auf **Eine Rolle löschen**.
   Das Dialogfeld Eine Benutzerrolle löschen wird geöffnet.
5. Wählen Sie die zu löschende Rolle aus und klicken Sie dann auf **OK**.

Einstellungen für die Benutzerverwaltung exportieren und importieren

Die Datenbank für die Benutzerverwaltung für die SCIEX OS Software kann exportiert und importiert werden. Nachdem Sie die Datenbank für die Benutzerverwaltung beispielsweise auf einem SCIEX Computer konfiguriert haben, exportieren Sie sie und importieren Sie sie dann auf andere SCIEX Computer, um sicherzustellen, dass die Einstellungen für die Benutzerverwaltung übereinstimmen.

Es werden nur Domänenbenutzer exportiert. Lokale Benutzer werden nicht exportiert.

Vor dem Importieren von Einstellungen für die Benutzerverwaltung sichert die Software automatisch die aktuellen Einstellungen. Der Benutzer kann die letzte Datensicherung wiederherstellen.

Einstellungen für die Benutzerverwaltung exportieren

1. Öffnen Sie den Arbeitsbereich „Konfiguration“.
2. Öffnen Sie die Seite „Benutzerverwaltung“.
3. Klicken Sie auf **Erweitert** > **Einstellungen für die Benutzerverwaltung exportieren**.
   Das Dialogfeld Einstellungen für die Benutzerverwaltung exportieren wird geöffnet.
4. Klicken Sie auf **Durchsuchen**.

5. Navigieren Sie zu dem Ordner, in dem die Einstellungen gespeichert werden sollen, wählen Sie ihn aus, und klicken Sie dann auf **Ordner auswählen**.
6. Klicken Sie auf **Exportieren**.
   Es wird eine Bestätigung mit dem Namen der Datei angezeigt, die die exportierten Einstellungen enthält.
7. Klicken Sie auf **OK**.

Einstellungen für die Benutzerverwaltung importieren

1. Öffnen Sie den Arbeitsbereich „Konfiguration“.
2. Öffnen Sie die Seite „Benutzerverwaltung“.
3. Klicken Sie auf **Erweitert** > **Einstellungen für die Benutzerverwaltung importieren**.
   Das Dialogfeld Einstellungen für die Benutzerverwaltung importieren wird geöffnet.
4. Klicken Sie auf **Durchsuchen**.
5. Navigieren Sie zu der Datei, die die zu importierenden Einstellungen enthält, wählen Sie sie aus, und klicken Sie dann auf **Öffnen**.
   Die Software überprüft, ob die Datei gültig ist.
6. Klicken Sie auf **Importieren**.
   Die Software sichert die aktuellen Einstellungen für die Benutzerverwaltung und importiert die neuen Einstellungen. Eine Bestätigung wird angezeigt.
7. Klicken Sie auf **OK**.

Einstellungen für die Benutzerverwaltung wiederherstellen

Vor dem Importieren von Einstellungen für die Benutzerverwaltung sichert die Software die aktuellen Einstellungen. Verwenden Sie dieses Verfahren, um die letzte Sicherung der Einstellungen für die Benutzerverwaltung wiederherzustellen.

1. Öffnen Sie den Arbeitsbereich „Konfiguration“.
2. Öffnen Sie die Seite „Benutzerverwaltung“.
3. Klicken Sie auf **Erweitert** > **Vorherige Einstellungen wiederherstellen**.
   Das Dialogfeld „Einstellungen für die Benutzerverwaltung wiederherstellen“ wird geöffnet.
4. Klicken Sie auf **Ja**.
5. Schließen Sie die SCIEX OS Software und öffnen Sie sie erneut.

Konfigurieren des Zugriffs auf Projekte und Projektdateien

Verwenden Sie die Windows-Sicherheitsfunktionen, um den Zugriff auf den Ordner „`SCIEX OS Data`“ zu steuern. Standardmäßig werden Projektdateien im Ordner „`SCIEX OS Data`“ gespeichert. Um auf ein Projekt zugreifen zu können, müssen die Benutzer Zugriff auf das

Stammverzeichnis haben, in dem die Projektdaten gespeichert sind. Weitere Informationen finden Sie im Abschnitt: Windows-Sicherheitskonfiguration.

Projektordner

Jedes Projekt umfasst Ordner, in denen verschiedene Arten von Dateien gespeichert sind. Für Informationen über die Inhalte der verschiedenen Ordner siehe die Tabelle: Tabelle 4-6.

Tabelle 4-6: Projektordner

Ordner	Inhalt
`\Acquisition Methods`	Enthält die im Projekt erstellten Massenspektrometer (MS)- und LC-Methoden. MS-Methoden haben die Erweiterung .msm und LC-Methoden die Erweiterung .lcm.
`\Audit Data`	Enthält die Projekt-Audit-Map und alle Audit-Aufzeichnungen.
`\Batch`	Enthält alle Erfassungschargendateien, die gespeichert wurden. Erfassungschargen haben die Erweiterung .bch.
`\Data`	Enthält die Dateien mit den Erfassungsdaten. Erfassungsdatendateien haben die Erweiterungen .wiff und .wiff2.
`\Project Information`	Enthält die Dateien für die Projektstandardeinstellungen.
`\Quantitation Methods`	Enthält alle Dateien mit den Verarbeitungsmethoden. Verarbeitungsmethoden haben die Erweiterung .qmethod.
`\Quantitation Results`	Enthält alle Dateien der Quantifizierungs-„Results Table“. „Results Table“-Dateien haben die Erweiterung .qsession.

Software-Dateitypen

Informationen über gängige Dateitypen in der SCIEX OS Software finden Sie in der Tabelle: Tabelle 4-7.

Tabelle 4-7: SCIEX OS-Dateien

Erweiterung	Dateityp	Ordner
`atds`	• Daten und Archive des Workstation-Audit-Trails • Einstellungen des Workstation-Audit-Trails • Daten und Archive des Projekt-Audit-Trails • Einstellungen des Projekt-Audit-Trails	• Für Projekte: *<project name>*`\Audit Data` • Für die Workstation: `C:\ProgramData\SCIEX\Audit Data`

Tabelle 4-7: SCIEX OS-Dateien (Fortsetzung)

Erweiterung	Dateityp	Ordner
atms	Audit-Maps	• Für Projekte: *<project name>*\Audit Data • Für die Workstation: C:\ProgramData\SCIEX\Audit Data
bch	Batch	Batch
cset	Einstellungen der Ergebnistabelle	Project Information
dad	Datei mit Massenspektrometriedaten	• Optimization • Data
exml	Standardeinstellungen des Projekts	Project Information
journal	Temporäre Dateien, die von der SCIEX OS Software erstellt werden	Verschiedene Ordner
lcm	LC-Methode	Acquisition Methods
msm	MS-Methode	Acquisition Methods
pdf	Daten im PDF-Format	—
qlayout	Arbeitsbereich-Layout	— **Hinweis:** Das übliche Arbeitsbereich-Layout für ein Projekt ist im Verzeichnis „Project Information“ gespeichert.
qmethod	Prozessierungsmethode	Quantitation Methods
qsession	Ergebnistabelle **Hinweis:** Die SCIEX OS Software kann nur qsession-Dateien öffnen, die mit der SCIEX OS Software erstellt wurden.	Quantitation Results

Tabelle 4-7: SCIEX OS-Dateien (Fortsetzung)

Erweiterung	Dateityp	Ordner
`wiff`	Datei mit Massenspektrometriedaten, die kompatibel ist mit der SCIEX OS Software **Hinweis:** Die SCIEX OS Software erstellt sowohl `wiff`- als auch `wiff2`-Dateien.	`Data`
`wiff.scan`	Datei mit Massenspektrometriedaten	• `Optimization` • `Data`
`wiff2`	Datei mit Massenspektrometriedaten, die von der SCIEX OS Software generiert wurde	• `Optimization` • `Data`
„`xls`“ oder „`xlsx`“	Excel-Tabelle	`Batch`
`xps`	Neukalibrierung	`Data\Cal`

Central Administrator Console 5

Die Central Administrator Console (CAC) Software ist eine optionale Alternative zur lokalen Verwaltung mit der SCIEX OS Software. Die CAC Software beinhaltet eine zentrale Verwaltung und Anpassung von Rollen, Benutzern, Workstations und Arbeitsgruppen in einer Anwendung.

Dieser Abschnitt beschreibt die CAC Software und erklärt, wie man diese zur zentralen Verwaltung von Personen, Projekten und Workstations konfiguriert und verwendet.

Hinweis: Um die CAC Software zu verwenden und Workstations am Server zu registrieren, muss sichergestellt werden, dass die SCIEX OS Software auf jeder Workstation installiert ist.

Die CAC Software wird per Lizenz aktiviert und kann auf jeder Workstation installiert werden, die SCIEX OS Version 3.0 und Windows Server 2019 unterstützt.

Die CAC Software ist im SCIEX OS Installationspaket enthalten. Die CAC Software und die SCIEX OS Software können jedoch nicht auf derselben Workstation installiert werden.

Benutzer

Verwenden Sie die Seite „Benutzerverwaltung“, um Windows-Benutzer und -Gruppen zur Datenbank für die Benutzerverwaltung für die SCIEX OS Software hinzuzufügen. Zudem kann der Administrator Benutzerrollen im Abschnitt „User Roles and Permissions“ hinzufügen, ändern und löschen. Für den Zugriff auf die Software müssen Benutzer in der Datenbank für die Benutzerverwaltung definiert sein oder müssen ein Mitglied einer in der Datenbank definierten Gruppen sein.

Benutzer-Pool

Ausschließlich autorisierte Benutzer können sich bei der Workstation anmelden und auf die SCIEX OS Software zugreifen, wenn die SCIEX OS Software mit der Central Administrator Console (CAC) Software verwaltet wird. Bevor Benutzer zu Arbeitsgruppen hinzugefügt werden können, müssen diese zum Benutzer-Pool hinzugefügt werden.

Benutzer oder Gruppe zum Benutzer-Pool hinzufügen

1. Öffnen Sie den Arbeitsbereich „Zentraladministration“.
2. Öffnen Sie die Seite „Benutzerverwaltung“.
3. Öffnen Sie die Registerkarte „Benutzer-Pool“.
4. Klicken Sie auf **Benutzer zum Benutzer-Pool hinzufügen** ().
   Das Dialogfeld „Benutzer oder Gruppen auswählen“ wird geöffnet.
5. Geben Sie den Namen des Benutzers oder der Gruppe ein und klicken Sie dann auf **OK**.

Tipp! Halten Sie die **Strg**-Taste gedrückt und klicken Sie dann auf **OK**, um mehrere Benutzer oder Gruppen auszuwählen.

Benutzer oder Gruppen löschen

1. Öffnen Sie den Arbeitsbereich „Zentraladministration“.
2. Öffnen Sie die Seite „Benutzerverwaltung“.
3. Öffnen Sie die Registerkarte „Benutzer-Pool“.
4. Wählen Sie im rechten Fensterbereich den zu löschenden Benutzer oder die zu löschende Gruppe aus und klicken Sie dann auf **Löschen**.
   Die Software fordert Sie zur Bestätigung auf.
5. Klicken Sie auf **OK**.

Benutzerrollen und Berechtigungen

In diesem Abschnitt wird die Seite „Benutzerrollen und Berechtigungen“ beschrieben.

Benutzer können einer oder mehreren vordefinierten Rollen, die in der folgenden Tabelle beschrieben werden, oder auch benutzerdefinierten Rollen zugewiesen werden, falls dies erforderlich ist. Die Funktionen, auf die der Benutzer zugreifen kann, werden durch Rollen angegeben. Die vordefinierten Rollen können nicht gelöscht und ihre Berechtigungen nicht geändert werden.

Hinweis: In der Central Administrator Console (CAC)-Software können Benutzer auch die früheste Version der SCIEX OS Software anzeigen, in der die Berechtigung unterstützt wird.

Tabelle 5-1: Vordefinierte Rollen

Rolle	Typische Aufgaben
Administrator	• Verwaltet das System • Konfiguriert die Sicherheit
Methodenentwickler	• Erstellt Methoden • Führt Batches aus • Analysiert Daten zur Verwendung durch den Benutzer
Analyst	• Führt Batches aus • Analysiert Daten zur Verwendung durch den Benutzer
Prüfer	• Prüft Daten • Prüft Audit-Trails • Bewertet Quantifizierungsergebnisse

Tabelle 5-2: Voreingestellte Berechtigungen

Berechtigung	Administrator	Methodenentwickler	Analyst	Prüfer
Batch				
Entsperrte Methoden zur Warteliste senden	✓	✓	✓	×
Öffnen	✓	✓	✓	✓
Speichern unter	✓	✓	✓	×
Zur Warteliste senden	✓	✓	✓	×
Speichern	✓	✓	✓	×
Ionenreferenztabelle speichern	✓	✓	✓	×
Daten-Unterordner hinzufügen	✓	✓	✓	×
Entscheidungsregeln konfigurieren	✓	✓	✓	×
Konfiguration				
Registerkarte „Allgemein“	✓	✓	×	×
Allgemein: Regionseinstellungen ändern	✓	✓	×	×
Allgemein: Vollbildmodus	✓	✓	×	×
Registerkarte „LIMS-Kommunikation“	✓	✓	×	×
Allgemein: Windows-Dienste stoppen	✓	×	×	×
Registerkarte „Audit-Maps“	✓	×	×	×
Registerkarte „Warteschlange“	✓	✓	✓	✓
Warteschlange: Geräteleerlaufzeit	✓	✓	×	×
Warteschlange: Maximale Anzahl erfasster Proben	✓	✓	×	×

Tabelle 5-2: Voreingestellte Berechtigungen (Fortsetzung)

Berechtigung	Administrator	Methodenentwickler	Analyst	Prüfer
Warteschlange: Andere Warteschlangeneinstellungen	✓	✓	×	×
Registerkarte „Projekte“	✓	✓	✓	✓
Projekte: Projekt erstellen	✓	✓	✓	×
Projekte: Eine Audit-Map-Vorlage auf ein bestehendes Projekt anwenden	✓	×	×	×
Projekte: Stammverzeichnis erstellen	✓	×	×	×
Projekte: Aktuelles Stammverzeichnis festlegen	✓	×	×	×
Projekte: Netzwerkanmeldedaten festlegen	✓	×	×	×
Projekte: Das Schreiben der Prüfsumme für die wiff-Datenerstellung aktivieren	✓	×	×	×
Projekte: Stammverzeichnis löschen	✓	×	×	×
Registerkarte „Geräte“	✓	✓	✓	×
Registerkarte „Benutzerverwaltung“	✓	×	×	×
Abmeldung des Benutzers erzwingen	✓	×	×	×
Registerkarte „CAC“[1]	✓	×	×	×

Tabelle 5-2: Voreingestellte Berechtigungen (Fortsetzung)

Berechtigung	Administrator	Methodenentwickler	Analyst	Prüfer
Registerkarte „Druckvorlagen“	✓	✓	×	×
Druckvorlagen: Druckvorlagen erstellen und modifizieren	✓	✓	×	×
Druckvorlagen: Standard-Druckvorlage festlegen	✓	✓	×	×
Druckvorlagen: Die aktuelle Vorlage auf alle Projekte im Stammverzeichnis anwenden	✓	×	×	×
Ereignisprotokoll				
Auf Arbeitsbereich „Ereignisprotokoll“ zugreifen	✓	✓	✓	✓
Protokoll archivieren	✓	✓	✓	✓
Audit-Trail				
Auf Arbeitsbereich „Audit-Trail“ zugreifen	✓	✓	✓	✓
Aktive Audit-Map anzeigen	✓	✓	✓	✓
Audit-Trail drucken/ exportieren	✓	✓	✓	✓
Feld „Datenerfassung“				
Start	✓	✓	✓	×
Stopp	✓	✓	✓	×
Speichern	✓	✓	✓	×
MS- und LC-Methode				

[1] In Version 3.1 wurde die Berechtigung **Zentraladministration aktivieren** umbenannt in **CAC**. Die Seite CAC im Arbeitsbereich „Konfiguration“ kann verwendet werden, um die Zentraladministration der SCIEX OS Software zu konfigurieren.

Tabelle 5-2: Voreingestellte Berechtigungen (Fortsetzung)

Berechtigung	Administrator	Methodenentwickler	Analyst	Prüfer
Auf Arbeitsbereich „Methode“ zugreifen	✓	✓	✓	✓
Neu	✓	✓	×	×
Öffnen	✓	✓	✓	✓
Speichern	✓	✓	×	×
Speichern unter	✓	✓	×	×
Methode sperren/ entsperren	✓	✓	×	×
Warteschlange				
Verwalten	✓	✓	✓	×
Start/Stopp	✓	✓	✓	×
Drucken	✓	✓	✓	✓
Probe bearbeiten	✓	✓	×	×
Bibliothek				
Auf Arbeitsbereich „Bibliothek“ zugreifen	✓	✓	✓	✓
MS Tune				
Auf Arbeitsbereich „MS Tune“ zugreifen	✓	✓	✓	×
Erweitertes MS-Tuning	✓	✓	×	×
Erweiterte Fehlerbehebung	✓	✓	×	×
Schnelle Statusüberprüfung	✓	✓	✓	×
Instrumentendaten wiederherstellen	✓	✓	×	×
Analyse				
Neue Ergebnisse	✓	✓	✓	×
Prozessierungsmethode erstellen	✓	✓	✓	×

Tabelle 5-2: Voreingestellte Berechtigungen (Fortsetzung)

Berechtigung	Administrator	Methodenentwickler	Analyst	Prüfer
Prozessierungsmethode ändern	✓	✓	×	×
Export nicht gesperrter Ergebnistabelle und Erstellen eines Berichts aus dieser erlauben	✓	×	×	×
Ergebnisse speichern für Automatisierungs-Batch	✓	✓	✓	×
Integrationsalgorithmus der standardmäßigen Quantifizierungsmethode ändern	✓	✓	×	×
Integrationsparameter der standardmäßigen Quantifizierungsmethode ändern	✓	✓	×	×
Warnung bei geänderten Peaks eines Projekts aktivieren	✓	×	×	×
Proben hinzufügen	✓	✓	✓	×
Ausgewählte Proben entfernen	✓	✓	✓	×
Externe Kalibrierung exportieren, importieren oder entfernen	✓	✓	✓	×
Probenname ändern	✓	✓	✓	×
Probentyp ändern	✓	✓	✓	×
Proben-ID ändern	✓	✓	✓	×
Ist-Konzentration ändern	✓	✓	✓	×

Tabelle 5-2: Voreingestellte Berechtigungen (Fortsetzung)

Berechtigung	Administrator	Methodenentwickler	Analyst	Prüfer
Verdünnungsfaktor ändern	✓	✓	✓	×
Kommentarfelder ändern	✓	✓	✓	×
Manuelle Integration aktivieren	✓	✓	✓	×
Peak auf „nicht gefunden“ setzen	✓	✓	✓	×
Einen Peak in die Ergebnistabelle einbeziehen oder aus dieser ausschließen	✓	✓	✓	×
Regressionsoptionen	✓	✓	✓	×
Integrationsparameter der Ergebnistabelle für ein einzelnes Chromatogramm ändern	✓	✓	✓	×
Quantifizierungsmethode für Komponente der Ergebnistabelle modifizieren	✓	✓	✓	×
Neue Einstellungen für metrische Darstellungen erstellen	✓	✓	✓	✓
Benutzerdefinierte Spalten hinzufügen	✓	✓	✓	×
Titelformat für die Peak-Überprüfung festlegen	✓	×	×	×
Benutzerdefinierte Spalte entfernen	✓	✓	×	×
Einstellungen für die Anzeige der Ergebnistabelle	✓	✓	✓	✓

Tabelle 5-2: Voreingestellte Berechtigungen (Fortsetzung)

Berechtigung	Administrator	Methodenentwickler	Analyst	Prüfer
Ergebnistabelle sperren	✓	✓	✓	✓
Ergebnistabelle entsperren	✓	×	×	×
Ergebnisdatei als „geprüft“ kennzeichnen und speichern	✓	×	×	✓
Berichtsvorlage ändern	✓	✓	×	×
Ergebnisse an LIMS übertragen	✓	✓	✓	×
Barcode-Spalte ändern	✓	✓	×	×
Zuweisung der Vergleichsprobe ändern	✓	✓	×	×
MSMS-Spektren zur Bibliothek hinzufügen	✓	✓	×	×
Standardeinstellungen des Projekts	✓	✓	×	×
Bericht in allen Formaten erstellen	✓	✓	✓	✓
Parameter für die Markierungskriterien bearbeiten	✓	✓	✓	×
Parameter für das automatische Entfernen von Ausreißern ändern	✓	✓	×	×
Automatische Entfernung von Ausreißern aktivieren	✓	✓	✓	×
Prozessierungsmethode über FF/LS aktualisieren	✓	✓	×	×

Tabelle 5-2: Voreingestellte Berechtigungen (Fortsetzung)

Berechtigung	Administrator	Methodenentwickler	Analyst	Prüfer
Ergebnisse über FF/LS aktualisieren	✓	✓	×	×
Funktion der Gruppierung nach Addukten aktivieren	✓	✓	×	×
Dateien suchen	✓	✓	✓	✓
Standardzugabe aktivieren	✓	✓	✓	×
Prozentsatzregel für die manuelle Integration festlegen	✓	×	×	×
Gewicht/Volumen ändern	✓	✓	✓	×
Explorer				
Auf Arbeitsbereich „Explorer“ zugreifen	✓	✓	✓	✓
Exportieren	✓	✓	✓	×
Drucken	✓	✓	✓	×
Optionen	✓	✓	✓	×
Erneut kalibrieren	✓	✓	×	×

Hinzufügen einer benutzerdefinierten Rolle

Die Central Administrator Console (CAC) Software verfügt über vier vordefinierte Rollen. Wenn weitere benötigt werden, dann kopieren Sie eine vorhandene Rolle und weisen Sie dieser Zugriffsrechte zu.

1. Öffnen Sie den Arbeitsbereich „Zentraladministration“.
2. Öffnen Sie die Seite „Benutzerverwaltung“.
3. Öffnen Sie die Registerkarte „Benutzerrollen und Berechtigungen“.
4. Klicken Sie auf **Rolle hinzufügen** ( ).
   Das Dialogfeld „Benutzerrolle duplizieren“ wird geöffnet.
5. Wählen Sie im Feld **Vorhandene Benutzerrolle** die Rolle aus, die als Vorlage für die neue Rolle verwendet werden soll.

6. Geben Sie einen Namen und eine Beschreibung für die Rolle ein und klicken Sie dann auf **OK**.
   Die neue Rolle wird im Fenster „Benutzerrollen und Berechtigungskategorien“ angezeigt.
7. Wählen Sie die Zugriffsberechtigungen für die Rolle aus, indem Sie die entsprechenden Kontrollkästchen aktivieren.
8. Klicken Sie auf **Alle Rollen speichern**.

Löschen einer benutzerdefinierten Rolle

1. Öffnen Sie den Arbeitsbereich „Zentraladministration“.
2. Öffnen Sie die Seite „Benutzerverwaltung“.
3. Öffnen Sie die Registerkarte „Benutzerrollen und Berechtigungen“.
4. Klicken Sie auf **Eine Rolle löschen**.
   Das Dialogfeld Eine Benutzerrolle löschen wird geöffnet.
5. Wählen Sie die zu löschende Rolle aus und klicken Sie dann auf **OK**.

Arbeitsgruppen

Verwenden Sie die Seite „Arbeitsgruppenverwaltung“ zum Verwalten von Arbeitsgruppen. Arbeitsgruppen umfassen Benutzer, Workstations und Projekte.

Erstellen Sie eine Arbeitsgruppe, indem Sie Ressourcen von ihren jeweiligen Pools hinzufügen. Bevor Sie Arbeitsgruppen erstellen, stellen Sie sicher, dass Sie alle potenziellen Nutzer zum „User Pool“, Workstations zum „Workstation Pool“ und Projektstammverzeichnisse zum „Project Pool“ hinzufügen.

Fügen Sie ggf. zusätzliche Rollen hinzu. Wählen Sie optional den Sicherheitsmodus für jede Arbeitsgruppe aus.

Die „Security Mode“-Einstellung für die Arbeitsgruppe hat Vorrang vor der „Security Mode“-Einstellung für die Workstation, wenn die Workstation bei der Central Administrator Console (CAC) Software registriert und Mitglied der Arbeitsgruppe ist.

Fügen Sie keine lokalen Benutzer zu Arbeitsgruppen hinzu. Die CAC Software ist eine Netzwerkanwendung und nur Netzwerkbenutzer sollten zu einer Arbeitsgruppe hinzugefügt werden.

Hinweis: In jeder Arbeitsgruppe sollte mindestens einem Benutzer Folgendes zugewiesen werden: Administrator-Rolle. Nur ein Administrator oder Supervisor kann den CAC Software-Bildschirm entsperren, wenn der aktuell angemeldete Benutzer nicht verfügbar ist.

Wenn Server-basierte Sicherheit für eine bestimmte Workstation nicht mehr erforderlich ist, dann verwalten Sie die Sicherheit für diese Workstation lokal über die SCIEX OS Software.

Erstellen einer Arbeitsgruppe

1. Öffnen Sie den Arbeitsbereich „Zentraladministration“.
2. Öffnen Sie die Seite „Arbeitsgruppenverwaltung“.

3. Klicken Sie auf **Arbeitsgruppe hinzufügen** ().
   Das Dialogfeld Eine Arbeitsgruppe hinzufügen wird geöffnet.
4. Geben Sie im Feld **Arbeitsgruppen-Name** einen Namen ein.
5. Geben Sie eine Beschreibung in das Feld **Beschreibung** ein und klicken Sie dann auf **Hinzufügen**.
   Die Arbeitsgruppe wird erstellt und dem Teilfenster „Arbeitsgruppen und Zuweisungen verwalten“ hinzugefügt. Die Central Administrator Console (CAC) Software erstellt die entsprechende Arbeitsgruppe auf dem Server.

Hinweis: „Integrated Mode“ ist die standardmäßige Sicherheitseinstellung.

Eine Arbeitsgruppe löschen

Wenn eine Arbeitsgruppe nicht länger benötigt wird, dann löschen Sie diese aus der Liste „Workgroup“. Das Löschen einer Arbeitsgruppe entfernt die Arbeitsgruppe nur aus der Central Administrator Console (CAC) Software. Auf der Workstation gehen keine Daten verloren.

1. Öffnen Sie den Arbeitsbereich „Zentraladministration“.
2. Öffnen Sie die Seite „Arbeitsgruppenverwaltung“.
3. Erweitern Sie die Liste **Arbeitsgruppen** und suchen Sie die zu löschende Arbeitsgruppe. Klicken Sie auf **Löschen**.
   Das Dialogfeld Arbeitsgruppe löschen wird geöffnet.
4. Klicken Sie auf **Ja**.

Benutzer oder Gruppen einer Arbeitsgruppe hinzufügen

Hinweis: Den zur Arbeitsgruppe hinzugefügten Benutzern wird nicht automatisch eine Rolle zugewiesen. Um Benutzern Rollen zuzuweisen, siehe Abschnitt: Hinzufügen oder Entfernen einer Rolle.

1. Öffnen Sie den Arbeitsbereich „Zentraladministration“.
2. Öffnen Sie die Seite „Arbeitsgruppenverwaltung“.
3. Erweitern Sie im Teilfenster „Arbeitsgruppen und Zuweisungen verwalten“ die Arbeitsgruppe, die geändert werden soll, und erweitern Sie dann die Liste **Benutzer**.
4. Wählen Sie einen Benutzer oder eine Gruppe aus und klicken Sie dann auf **Hinzufügen** ().

Tipp! Sie können mehrere Benutzer hinzufügen oder auswählen, indem Sie die **Umschalttaste** drücken und dann die gewünschten Benutzer auswählen.

Der Benutzer bzw. die Gruppe wird zur aktuellen Arbeitsgruppe hinzugefügt.

5. Weisen Sie dem hinzugefügten Benutzer bzw. der Gruppe eine oder mehrere Rollen zu. Siehe Abschnitt: Hinzufügen oder Entfernen einer Rolle.
6. Klicken Sie auf **Speichern**.

Hinzufügen oder Entfernen einer Rolle

Voraussetzungen
• Benutzer oder Gruppen einer Arbeitsgruppe hinzufügen.

Informationen über das Erstellen von Rollen in der Central Administrator Console (CAC) Software finden Sie im Abschnitt: Hinzufügen einer benutzerdefinierten Rolle. Benutzer oder Gruppen mit einer zugewiesenen Rolle besitzen alle der Rolle zugeordneten Berechtigungen. Benutzer oder Gruppen können über mehr als eine Rolle gleichzeitig verfügen.

1. Öffnen Sie den Arbeitsbereich „Zentraladministration“.
2. Öffnen Sie die Seite „Arbeitsgruppenverwaltung“.
3. Erweitern Sie im Teilfenster „Arbeitsgruppen und Zuweisungen verwalten“ die Arbeitsgruppe, die geändert werden soll, und erweitern Sie dann die Liste **Benutzer**.
4. Im Abschnitt „Aktuelle Arbeitsgruppen-Mitgliedschaft“ können Sie Rollen in der Spalte **Rollen zuweisen** zuweisen oder entfernen.
5. Klicken Sie auf **Speichern**.

Workstations einer Arbeitsgruppe hinzufügen

Hinweis: Eine Workstation wird im Workstation Pool nur dann angezeigt, wenn sie bei der Central Administrator Console (CAC) Software registriert ist. Siehe Abschnitt: Hinzufügen einer Workstation

1. Öffnen Sie den Arbeitsbereich „Zentraladministration“.
2. Öffnen Sie die Seite „Arbeitsgruppenverwaltung“.
3. Erweitern Sie im Teilfenster „Arbeitsgruppen und Zuweisungen verwalten“ die Arbeitsgruppe, die geändert werden soll, und erweitern Sie dann die Liste **Workstations**.
4. Wählen Sie eine Workstation aus und klicken Sie dann auf **Hinzufügen** (). Die Workstation wird zur aktuellen Arbeitsgruppe hinzugefügt.
5. Klicken Sie auf **Speichern**.

Arbeitsgruppen-Sicherheitseinstellungen zuweisen

Voraussetzungen
• Hinzufügen einer Workstation • Workstations einer Arbeitsgruppe hinzufügen

Informationen über Sicherheitsmodi finden Sie im Abschnitt: Konfigurieren des Sicherheitsmodus.

1. Öffnen Sie den Arbeitsbereich „Zentraladministration“.
2. Öffnen Sie die Seite „Arbeitsgruppenverwaltung“.
3. Erweitern Sie im Teilfenster „Arbeitsgruppen und Zuweisungen verwalten“ die Arbeitsgruppe, die geändert werden soll, und erweitern Sie dann die Liste **Workstations**.
4. (Optional) Um die aktuelle Arbeitsgruppe als Standard-Arbeitsgruppe für diese Workstation festzulegen, aktivieren Sie das Kontrollkästchen **Standardwert festlegen** im Abschnitt „Aktuelle Arbeitsgruppen-Mitgliedschaft“.
5. Wählen Sie im Abschnitt „Sicherheitseinstellungen zuweisen“ den **Sicherheitsmodus** für die Arbeitsgruppe aus und geben Sie dann die entsprechenden Zeiten für **Bildschirmsperre** und **Automatische Abmeldung** ein.
6. Klicken Sie auf **Speichern**.

Projekte einer Arbeitsgruppe hinzufügen

Hinweis: Dieses Verfahren ist nur erforderlich, wenn der Projektzugriff zentral verwaltet wird.

Hinweis: Wenn ein Projekt zu mehr als einer Arbeitsgruppe hinzugefügt wird, dann werden die Benutzerberechtigungen für das Projekt angehängt aber nicht überschrieben. Zum Beispiel enthält Workgroup 1 den User A, User B und das Project_01. Workgroup 2 enthält den User B und User C. Wenn Project_01 zur Workgroup 2 hinzugefügt wird, dann erhalten User A, User B und User C Zugriff auf das Project_01.

1. Öffnen Sie den Arbeitsbereich „Zentraladministration“.
2. Öffnen Sie die Seite „Arbeitsgruppenverwaltung“.
3. Erweitern Sie im Teilfenster „Arbeitsgruppen und Zuweisungen verwalten“ die Arbeitsgruppe, die geändert werden soll, und erweitern Sie dann die Liste **Projekte**.
4. Aktivieren Sie das Kontrollkästchen **Zentralisierte Einstellungen für Projekte verwenden**.
   Der Abschnitt zur Projektauswahl wird angezeigt.
5. Wählen Sie ein **Projekt-Stammverzeichnis** aus, um eine ganze Projektgruppe hinzuzufügen oder erweitern Sie den Projektstamm und wählen Sie ein bestimmtes Projekt zum Hinzufügen zur Arbeitsgruppe aus.

6. Klicken Sie auf **Hinzufügen** (), um die Projekte zur Arbeitsgruppe hinzuzufügen. Der Projektstamm wird zur Tabelle „Aktuelle Arbeitsgruppen-Mitgliedschaft“ hinzugefügt. Erweitern Sie den Projektstamm, um die aktuellen Projekte in der Arbeitsgruppe anzuzeigen.
7. Klicken Sie auf **Speichern**.

Projekte verwalten

Verwenden Sie die Seite „Projektmanagement“ zum Erstellen, Ändern und Löschen von Projekten.

Um auf ein Projekt zugreifen zu können, müssen die Benutzer Zugriff auf das Stammverzeichnis haben, in dem die Projektdaten gespeichert sind. Weitere Informationen finden Sie im Abschnitt: Über Projekte und Stammverzeichnisse.

Über Projekte und Stammverzeichnisse

Ein Stammverzeichnis ist ein Ordner, der ein oder mehrere Projekte enthält. Dies ist der Ordner, in dem die Software nach Projektdaten sucht. Das vordefinierte Stammverzeichnis ist `D:\SCIEX OS Data`.

Um sicherzustellen, dass Projektinformationen sicher gespeichert werden, erstellen Sie Projekte mithilfe der Central Administrator Console (CAC) Software. Fügen Sie Projekte zum „Projektstamm-Pool“ hinzu, bevor Sie sie zu einer Arbeitsgruppe hinzufügen. Siehe Abschnitt: Hinzufügen eines Projekts.

Projektdaten können in Unterordnern organisiert werden. Erstellen Sie die Unterordner mit der CAC Software. Siehe Abschnitt: Hinzufügen eines Unterordners.

Hinweis: Wenn ein Projekt außerhalb der CAC Software erstellt wird, dann sollte der Projektstamm nach dem Erstellen des Projekts aktualisiert werden. Wenn der Stamm aktualisiert wird, dann werden die Inhalte des „Projektstamm-Pool“ mit dem Inhalt der Projekt-Stammverzeichnisse im Netzwerk synchronisiert.

Hinzufügen eines Stammverzeichnisses

Ein Stammverzeichnis ist der Ordner, in dem ein oder mehrere Projekte gespeichert werden.

Hinweis: Die Software speichert bis zu zehn Stammverzeichnisse.

Tipp! Lokale Laufwerke sind nicht über das Netzwerk zugänglich. Ein Stammverzeichnis kann nur auf einem freigegebenen Laufwerk erstellt werden.

1. Öffnen Sie den Arbeitsbereich „Zentraladministration“.
2. Öffnen Sie die Seite „Projektmanagement“.
3. Klicken Sie auf **Neuen oder vorhandenen Projektstamm zum Projekt-Pool hinzufügen** ().

Das Dialogfeld „Stammverzeichnis hinzufügen“ wird geöffnet.

4. Geben Sie den vollständigen Pfad zum Stammverzeichnis ein und klicken Sie dann auf **OK**.
   Der Ordner wird erstellt.

   Tipp! Statt den Pfad einzugeben, klicken Sie auf **Durchsuchen** und wählen Sie den Ordner aus, in dem das Stammverzeichnis erstellt werden soll.

   Tipp! Erstellen Sie alternativ einen Ordner im Datei-Explorer, suchen Sie diesen Ordner und wählen Sie ihn aus.

   Hinweis: Bei Installationen der SCIEX OS Software mit einer Prozessierungslizenz kann das Stammverzeichnis ein Ordner der Analyst Software (`Analyst Data\Projects`) sein.

5. Klicken Sie auf **OK**.
   Das neue Stammverzeichnis wird zum Stammverzeichnis für das aktuelle Projekt.

Löschen eines Projekt-Stammverzeichnisses

Die Software führt eine Liste der letzten zehn verwendeten Stammverzeichnisse. Der Benutzer kann Stammverzeichnisse aus dieser Liste löschen.

Hinweis: Durch das Löschen eines Projekt-Stammverzeichnisses werden ebenfalls alle zugehörigen Projekte aus dem Projektstammpool gelöscht.

1. Öffnen Sie den Arbeitsbereich „Zentraladministration“.
2. Öffnen Sie die Seite „Projektmanagement“.
3. Suchen Sie das zu löschende Projekt-Hauptverzeichnis und klicken Sie dann auf **Projektstamm löschen** im Abschnitt „Aktionen“.
   Die Software fordert Sie zur Bestätigung auf.
4. Klicken Sie auf **OK**.

Hinzufügen eines Projekts

Voraussetzungen
• Hinzufügen eines Stammverzeichnisses

Im Projekt werden Erfassungsmethoden, Daten, Chargen, Verarbeitungsmethoden, Verarbeitungsergebnisse usw. gespeichert. Wir empfehlen, einen separaten Projektordner für jedes Projekt zu verwenden.

Außerhalb der Central Administrator Console (CAC) Software sollten Sie keine Projekte erstellen oder Dateien kopieren oder einfügen.

1. Öffnen Sie den Arbeitsbereich „Zentraladministration“.

2. Öffnen Sie die Seite „Projektmanagement“.
3. Klicken Sie auf **Projekt hinzufügen** im Abschnitt „Aktionen“ des Stammordners.
   Das Dialogfeld „Neues Projekt“ wird geöffnet.
4. Geben Sie den Projektnamen ein.
5. Klicken Sie auf **OK**.
   Das neue Projekt wird unter dem Projektstamm angezeigt.

Hinzufügen eines Unterordners

Daten in Projekten können in Unterordnern weitergehend organisiert werden.

1. Öffnen Sie den Arbeitsbereich „Zentraladministration“.
2. Öffnen Sie die Seite „Projektmanagement“.
3. Klicken Sie auf **Daten-Unterordner hinzufügen** im Abschnitt „Aktionen“ des Stammordners.
   Das Dialogfeld „Daten-Unterordner hinzufügen“ wird geöffnet.
4. Wählen Sie ein Projekt aus, zu dem der Unterordner gehören soll.
5. Klicken Sie auf **Neuen Daten-Unterordner hinzufügen** ( ).
   Das Dialogfeld „Name des Daten-Unterordners“ wird geöffnet.
6. Geben Sie den Namen des Unterordners ein.
7. Klicken Sie auf **Speichern**.

Tipp! Unterordner können innerhalb anderer Unterordner geschachtelt werden. Um einen geschachtelten Unterordner zu erstellen, wählen Sie einen vorhandenen Unterordner im Abschnitt „Projekt-Daten-Unterordner“ aus und klicken Sie dann auf **Neuen Daten-Unterordner hinzufügen** ( ).

8. Schließen Sie das Dialogfeld „Daten-Unterordner hinzufügen“.

Workstations

Verwenden Sie die Seite „Workstation-Verwaltung“ zum Verwalten sämtlicher mit der CAC Software verbundenen Workstations. Auf Workstations, die über die CAC Software gesteuert werden, werden automatisch benutzerdefinierte Einstellungen angewendet.

Hinzufügen einer Workstation

Auf der Seite Workstation-Verwaltung können Administratoren Workstations hinzufügen, die zentrale Steuerung von Workstations aktivieren und deaktivieren sowie Workstations entfernen.

1. Öffnen Sie den Arbeitsbereich „Zentraladministration“.

2. Öffnen Sie die Seite „Workstation-Verwaltung“.
3. Klicken Sie auf **Workstation zum Workstation-Pool hinzufügen** ().
   Das Dialogfeld „Computer auswählen“ wird geöffnet.
4. Geben Sie die Namen der Workstations ein, die hinzugefügt werden sollen, und klicken Sie dann auf **OK**.
   Der **Status** der Zentraladministration der Workstation ändert sich von **Verbindung wird hergestellt** in **Deaktiviert**.
5. (Optional) So aktivieren Sie die zentrale Steuerung der Workstation:
   a. Klicken Sie in der Spalte „**Status**“ auf **Deaktiviert**.
   b. Klicken Sie auf **OK**.

Tipp! Benutzer können zudem die Zentraladministration in der SCIEX OS Software aktivieren. Siehe das Dokument: *SCIEX OS Software Hilfesystem*.

Löschen einer Workstation

Wird eine Workstation nicht mehr gebraucht oder ist in einer Arbeitsgruppe nicht mehr erforderlich, dann löschen Sie diese aus dem „Workstation Pool“. Wird eine Workstation gelöscht, dann wird diese aus allen Arbeitsgruppen entfernt, denen sie zugewiesen wurde. Auf der Workstation gehen keine Daten verloren, wenn sie entfernt wird.

1. Öffnen Sie den Arbeitsbereich „Zentraladministration“.
2. Öffnen Sie die Seite „Workstation-Verwaltung“.
3. Klicken Sie auf **Workstation-Verwaltung**.
4. Suchen Sie im Teilfenster „Workstation-Pool“ die zu löschende Workstation und klicken Sie dann auf **Löschen**.
   Das Dialogfeld „Workstation löschen“ wird geöffnet.
5. Klicken Sie auf **OK**.

Berichte und Sicherheitsfunktionen

Erstellen von Datenberichten

Erstellen Sie mit diesem Verfahren Datenberichte, die Details zu konfigurierten Benutzern, Rollen, Workstations, Projekten und Arbeitsgruppen enthalten.

1. Öffnen Sie den Arbeitsbereich „Zentraladministration“.
2. Klicken Sie auf **Drucken**.
   Das Dialogfeld „Druckoptionen“ wird geöffnet.
3. Zu druckende Seiten auswählen und klicken Sie dann auf **Fortsetzen**.
4. Stellen Sie die Druckoptionen ein und klicken Sie dann auf **Drucken**.

5. (Nur als PDF drucken) Navigieren Sie zu dem Speicherort, an dem der Bericht gespeichert werden soll und klicken Sie dann auf **Speichern**.

Exportieren der Einstellungen für die CAC Software

Verwenden Sie dieses Verfahren, um Sicherheitseinstellungen zu exportieren, damit sie in ein anderes Central Administrator Console (CAC) System importiert werden können. Die Einstellungen werden als eine `ecac`-Datei exportiert.

1. Öffnen Sie den Arbeitsbereich „Zentraladministration“.
2. Klicken Sie auf **Erweitert** > **CAC-Einstellungen exportieren**.
   Das Dialogfeld „CAC-Einstellungen exportieren“ wird geöffnet.
3. Klicken Sie auf **Durchsuchen**.
4. Navigieren Sie zu dem Ordner, in dem die Einstellungen gespeichert werden sollen, wählen Sie ihn aus, und klicken Sie dann auf **Ordner auswählen**.
5. Klicken Sie auf **Exportieren**.
   Es wird eine Bestätigung mit dem Namen der Datei angezeigt, die die exportierten Einstellungen enthält.
6. Klicken Sie auf **OK**.

Importieren der Einstellungen der CAC Software

Voraussetzungen
• Exportieren der Einstellungen für die CAC Software

Verwenden Sie dieses Verfahren, um Sicherheitseinstellungen aus anderen Central Administrator Console (CAC) Systemen zu importieren. Die Einstellungen werden aus einer `ecac`-Datei importiert.

1. Öffnen Sie den Arbeitsbereich „Zentraladministration“.
2. Öffnen Sie den Arbeitsbereich „Konfiguration“.
3. Öffnen Sie die Seite „Benutzerverwaltung“.
4. Klicken Sie auf **Erweitert** > **CAC-Einstellungen importieren**.
   Das Dialogfeld „CAC-Einstellungen importieren“ wird geöffnet.
5. Klicken Sie auf **Durchsuchen**.
6. Navigieren Sie zu der Datei, die die zu importierenden Einstellungen enthält, wählen Sie sie aus, und klicken Sie dann auf **Öffnen**.
   Die Software stellt sicher, dass die Datei gültig ist.
7. Klicken Sie auf **Importieren**.
   Die Software sichert die aktuellen Einstellungen und importiert die neuen Einstellungen. Eine Bestätigung wird angezeigt.

Hinweis: Die importierten Einstellungen werden nach dem Neustart der Software übernommen.

8. Klicken Sie auf **OK**.

Wiederherstellen der Einstellungen der CAC-Software

Verwenden Sie dieses Verfahren, um die zuletzt exportierten `ecac`-Einstellungen automatisch zu importieren.

1. Öffnen Sie den Arbeitsbereich „Zentraladministration“.
2. Klicken Sie auf **Erweitert** > **CAC-Einstellungen wiederherstellen**.
   Das Dialogfeld „CAC-Einstellungen wiederherstellen“ wird geöffnet.

   Hinweis: Die wiederhergestellten Einstellungen werden nach dem Neustart der Central Administrator Console (CAC) Software übernommen.

3. Klicken Sie auf **Ja**.

Einstellungen für die CAC Benutzerverwaltung exportieren

Verwenden Sie dieses Verfahren, um Einstellungen für die Benutzerverwaltung zu exportieren, die auf eine anderes Central Administrator Console (CAC)-System angewendet werden können. Die Einstellungen werden als eine `data`-Datei exportiert.

Hinweis: Exportierte Einstellungen können nur in ein System importiert werden, das die gleiche Version der CAC Software verwendet.

1. Öffnen Sie den Arbeitsbereich „Konfigurationsverwaltung“.
2. Klicken Sie auf **Erweitert** > **Einstellungen für die Benutzerverwaltung exportieren**.
   Das Dialogfeld „CAC-Einstellungen exportieren“ wird geöffnet.
3. Klicken Sie auf **Durchsuchen**.
4. Navigieren Sie zu dem Ordner, in dem die Einstellungen gespeichert werden sollen, wählen Sie ihn aus, und klicken Sie dann auf **Ordner auswählen**.
5. Klicken Sie auf **Exportieren**.
   Es wird eine Bestätigung mit dem Namen der Datei angezeigt, die die exportierten Einstellungen enthält.
6. Klicken Sie auf **OK**.

Einstellungen für die CAC Benutzerverwaltung importieren

Voraussetzungen
• Einstellungen für die CAC Benutzerverwaltung exportieren

Verwenden Sie dieses Verfahren, um Sicherheitseinstellungen aus einem anderen Central Administrator Console (CAC)-System zu importieren. Diese Einstellungen werden aus einer `data`-Datei importiert.

Hinweis: Exportierte Einstellungen können nur in ein System importiert werden, das die gleiche Version der CAC Software verwendet.

1. Öffnen Sie den Arbeitsbereich „Konfigurationsverwaltung“.
2. Klicken Sie auf **Erweitert** > **Einstellungen für die Benutzerverwaltung importieren**.
   Das Dialogfeld „Einstellungen für die Benutzerverwaltung importieren“ wird geöffnet.
3. Klicken Sie auf **Durchsuchen**.
4. Navigieren Sie zu der Datei, die die zu importierenden Einstellungen enthält, wählen Sie sie aus, und klicken Sie dann auf **Öffnen**.
   Die Software stellt sicher, dass die Datei gültig ist.
5. Klicken Sie auf **Importieren**.
   Die Software sichert die aktuellen Einstellungen und importiert die neuen Einstellungen. Eine Bestätigung wird angezeigt.

   Hinweis: Die importierten Einstellungen werden nach dem Neustart der CAC Software übernommen.
6. Klicken Sie auf **OK**.

Netzwerkerfassung 6

Dieser Abschnitt beschreibt, wie die Netzwerkerfassung in der SCIEX OS Software funktioniert. Zudem werden die Vorteile und Einschränkungen von netzwerkbasierten Projekten behandelt. Darüber hinaus werden auch Verfahren für die Konfiguration der Netzwerkerfassung beschrieben.

Über die Netzwerkerfassung

Die Netzwerkerfassung kann verwendet werden, um Daten aus einem oder mehreren Gerät(en) in netzwerkbasierten Projektordnern zu erfassen, die auf Remote-Arbeitsplätzen verarbeitet werden können. Dieser Prozess ist Netzwerkfehlern gegenüber tolerant und stellt sicher, dass keine Daten verloren gehen, wenn die Netzwerkverbindung während der Erfassung ausfällt.

Bei der Verwendung von Netzwerkprojekten kann die Systemleistung langsamer sein als bei der Verwendung lokaler Projekte. Da sich in den Netzwerkordnern auch einige Audit-Trails befinden, ist jede Aktion, die eine Projekt-Audit-Aufzeichnung erstellt, ebenfalls langsamer. Abhängig von der Netzwerkleistung kann das Öffnen von Netzwerkdateien einige Zeit beanspruchen. Die Netzwerkleistung hängt nicht nur mit der physischen Netzwerk-Hardware zusammen, sondern auch mit dem Netzwerk-Traffic und -Design.

Hinweis: Wenn der ClearCore2-Dienst während der Netzwerkerfassung unterbrochen wird, werden die partiellen Probendaten der zu erfassenden Probe zum Zeitpunkt der Unterbrechung nicht in die Datendatei geschrieben.

Hinweis: Wenn Sie eine Netzwerkerfassung in einer regulierten Umgebung verwenden, synchronisieren Sie die Uhrzeit des Computers mit der Uhrzeit des Servers, um genaue Zeitstempel zu erhalten. Die Serverzeit wird für die Erstellungszeit der Datei verwendet. Der „Audit Trail Manager“ zeichnet die Erstellungszeit der Datei über die lokale Computerzeit auf.

VORSICHT: Möglicher Datenverlust. Speichern Sie die Aufzeichnungsdaten mehrerer Erfassungscomputer nicht in derselben Netzwerkdatendatei.

Vorteile der Netzwerkerfassung

Die Datenerfassung im Netzwerk bietet eine sichere Methode, mit Projektordnern zu arbeiten, die sich vollständig auf Netzwerkservern befinden. Dies reduziert die Komplexität beim lokalen Erfassen von Daten und beim anschließenden Verschieben der Daten an einen Netzwerkstandort zur Speicherung. Da Netzlaufwerke normalerweise automatisch gesichert werden, wird außerdem die Notwendigkeit zur Sicherung lokaler Laufwerke reduziert oder eliminiert.

Sicheres Netzwerkkonto

In einer regulierten Umgebung, in der Daten in einem Netzwerkordner erfasst werden, wird dringend empfohlen, dass Benutzer über keine Berechtigungen zum Löschen für den Zielordner verfügen. Ohne Berechtigungen zum Löschen für diesen Ordner kann die SCIEX OS Software jedoch nicht die optimale Leistung erzielen. Über die SNA-Funktion (Secure Network Account, sicheres Netzwerkkonto) wird ein Netzwerkkonto identifiziert, das uneingeschränkte Dateiberechtigungen für das Netzwerk-Stammverzeichnis besitzt. Der ClearCore2-Dienst verwendet dieses Konto zum Übertragen von Daten in den Netzwerkordner.

Das SNA muss über einen Vollzugriff verfügen für:

- Den Netzwerkstammverzeichnis-Ordner
- Den Ordner `SCIEX OS Data\NetworkBackup` auf dem Erfassungscomputer
- Den Ordner `SCIEX OS Data\TempData` auf dem Erfassungscomputer

Folgendes ist für das SNA nicht erforderlich:

- Es muss nicht zur Administratorgruppe auf dem Computer gehören.
- Es muss nicht in der Benutzerverwaltungsdatenbank für die SCIEX OS Software vorhanden sein.

Das SNA wird auf der Seite „Projekte“ im Arbeitsbereich „Konfiguration“ festgelegt. Es kann nur ein gültiges Windows Netzwerk oder Domänenkonto angegeben werden.

Wenn kein SNA festgelegt ist, dann verwendet die SCIEX OS Software die Anmeldedaten des aktuell angemeldeten Benutzers, um die Daten in das Stammverzeichnis des Netzwerks zu übertragen. Damit der Transfer erfolgreich ist, muss das Konto über Schreibzugriff auf alle Projektordner verfügen, in denen Daten erfasst werden, und zwar ungeachtet dessen, welcher Benutzer den Batch zur Erfassung übermittelt hat.

Datentransferprozess

Wenn die SCIEX OS Software Daten in einem Speicherplatz im Netzwerk erfasst, wird jede Probe zunächst in einem Ordner auf dem lokalen Laufwerk gespeichert und dann in das Netzwerk übertragen. Wenn der erfolgreiche Transfer der gesamten Datendatei bestätigt wurde, wird der lokale Ordner, der die Daten enthält, gelöscht. Sollte das Netzwerk während des Prozesses nicht mehr verfügbar sein, versucht die SCIEX OS Software es alle 15 Minuten erneut, bis der Transfer erfolgreich ist.

Informationen über den Datenzugriff während einer längeren Unterbrechung der Netzwerkverbindung finden Sie im Abschnitt: Entfernen von Proben aus einem Netzwerktransfer-Ordner.

Konfigurieren der Netzwerkerfassung

Ein Stammverzeichnis ist der Ordner, in dem die SCIEX OS Software Daten speichert. Um sicher zu sein, dass Informationen zum Projekt sicher gespeichert werden, erstellen Sie

das Stammverzeichnis mit der SCIEX OS Software. Erstellen Sie keine Projekte in Windows-Explorer.

Wenn Sie, optional, Stammverzeichnisse in einer Netzwerkressource erstellen, legen Sie die „**Anmeldedaten für sicheres Netzwerkkonto**“ fest. Es handelt sich hierbei um das in der Netzwerkressource definierte sichere Netzwerkkonto. Siehe Abschnitt: Sicheres Netzwerkkonto.

Informationen zum Erstellen von Projekten und Teilprojekten finden Sie im Dokument: *SCIEX OS-Software-Benutzerhandbuch*.

Spezifizieren eines sicheren Netzwerkkontos

Wenn Projekte in einer Netzwerkressource gespeichert werden, kann ein sicheres Netzwerkkonto spezifiziert werden, um sicherzustellen, dass alle Benutzer der Workstation über den erforderlichen Zugriff auf die Netzwerkressource verfügen.

1. Öffnen Sie den Arbeitsbereich „Konfiguration“.
2. Klicken Sie auf **Projekte**.
3. Klicken Sie im Abschnitt **Erweitert** auf **Anmeldedaten für sicheres Netzwerkkonto**.
4. Geben Sie den Benutzernamen, das Passwort und die Domäne für das in der Netzwerkressource definierte sichere Netzwerkkonto ein.
5. Klicken Sie auf **OK**.

Auditing 7

In diesem Abschnitt wird die Verwendung der Auditing-Funktion beschrieben. Informationen über Windows-Auditing-Funktionen finden Sie im Abschnitt: System-Audits.

Audit-Trails

Die Software unterteilt Audit-Ereignisse im Arbeitsbereich „Audit-Trail“. Die Software speichert die Ereignisse in Audit-Trails. Hierbei handelt es sich um Dateien, die die Aufzeichnungen von geprüften Ereignissen speichern.

Workstation-Ereignisse werden im Audit-Trail der Workstation gespeichert. Workstation-Audit-Trails sind Dateien, die die geprüften Ereignisse für den Computer speichern, auf dem die SCIEX OS Software installiert ist.

CAC-Systemereignisse werden im CAC-Audit-Trail gespeichert.

Projektereignisse werden im Audit-Trail des Projekts gespeichert. Im Arbeitsbereich „Audit-Trail“ werden die Audit-Trails für die Projekte im aktiven Stammverzeichnis angezeigt. Prozessierungs-Audit-Trail-Ereignisse sind im Projekt-Audit-Trail enthalten und werden gemeinsam mit der Ergebnistabelle gespeichert.

Eine vollständige Liste der geprüften Ereignisse finden Sie im Abschnitt: Audit-Ereignisse.

Audit-Trails bilden in Verbindung mit Dateien, wie z. B. `.wiff2`- und Ergebnistabellen-Dateien, gültige elektronische Aufzeichnungen, die für Compliance-Zwecke verwendet werden können.

Tabelle 7-1: -Audit-Trails

Audit-Trail	Beispiele für aufgezeichnete Ereignisse	Verfügbare Audit-Maps (Speicherort)	Standard-Audit-Maps

Workstation (SCIEX OS)	• Änderungen an:
	  • Zuweisung der aktiven Audit-Map
	  • Geräte-Tuning
	  • Probenwartesc hlangen
	  • Sicherheit
	  • Tuning
	  • Geräte
		• Ordner `C:\ProgramDat a\SCIEX\Audit Data`	• No Audit Map

Tabelle 7-1: -Audit-Trails (Fortsetzung)

Audit-Trail	Beispiele für aufgezeichnete Ereignisse	Verfügbare Audit-Maps (Speicherort)	Standard-Audit-Maps

CAC	• Änderungen an:
	  • Audit-Map
	  • CAC
	  • Sicherheit
	  • Benutzerprotokoll
		• Ordner `C:\ProgramData\SCIEX\Audit Data`	• Silent Audit Map

Projekt (1x pro Projekt)	• Änderungen an:
	  • Zuweisung der aktiven Audit-Map (SCIEX OS)
	  • Projekt
	  • Daten
	• Drucken
		• Ordner `<project>\Audit Data`	• Spezifiziert auf der Seite „Audit-Maps“ des Arbeitsbereichs „Konfiguration“

Sobald ein Audit-Trail 20.000 Audit-Aufzeichnungen enthält, archivieren die SCIEX OS und die CAC Software diese Aufzeichnungen automatisch und es beginnt ein neuer Audit-Trail. Weitere Informationen finden Sie im Abschnitt: Audit-Trail-Archive.

Audit-Maps

Eine Audit-Map ist eine Datei, die eine Liste aller Ereignisse enthält, die geprüft werden können, sowie Informationen dazu, ob ein Änderungsgrund oder eine elektronische Signatur für das Ereignis erforderlich ist. In der SCIEX OS Software stehen die beiden folgenden Audit-Maps zur Verfügung: Workstation und Projekt. In der CAC Software stehen die beiden folgenden Audit-Maps zur Verfügung: CAC und Projekt.

Workstation-Audit-Maps steuern die Ereignisse, die auf einer Workstation geprüft werden.

Project Audit Maps steuern die Ereignisse, die für ein Projekt geprüft werden und im Projektordner gespeichert werden.

Hinweis: Die Audit-Map für ein Projekt kann in der SCIEX OS Software oder in der Central Administrator Console (CAC)-Software bearbeitet werden.

Der Benutzer kann viele Audit-Maps erstellen. Für jede Workstation, jedes CAC-System und jedes Projekt kann jedoch zeitgleich immer nur eine Audit-Map verwendet werden. Die für

eine Workstation, ein CAC-System oder ein Projekt verwendete Audit-Map wird als aktive Audit-Map bezeichnet.

Wenn die SCIEX OS Software installiert ist, dann ist die Standard-Audit-Map für alle neuen Projekte „Keine Audit-Map“. Wenn die CAC Software installiert ist, dann ist die Standard-Audit-Map für alle neuen Projekte „Silent Audit-Map“.Der Benutzer kann eine andere aktive Audit-Map als Standard für alle neuen Projekte angeben. Siehe Abschnitt: Ändern einer aktiven Audit-Map für ein Projekt.

Einrichten von Audit-Maps

Bevor Sie mit zu auditierenden Projekten arbeiten können, müssen Sie auf Standardarbeitsanweisungen anwendbare Audit-Maps konfigurieren. Es stehen nach der Installation der Software zwar mehrere standardmäßige Audit-Map-Vorlagen zur Verfügung, Sie müssen jedoch möglicherweise eine benutzerdefinierte Map erstellen. Stellen Sie sicher, dass eine Audit-Map für die Workstation oder den CAC-Audit-Trail und eine Audit-Map für jedes Projekt verfügbar ist.

Tabelle 7-2: Checkliste für das Konfigurieren von Auditing

Aufgabe	Siehe

• SCIEX OS: Erstellen Sie eine Audit-Map für den Workstation-Audit-Trail.
• CAC Software: Erstellen Sie eine Audit-Map für den CAC-Audit-Trail.
	• SCIEX OS:
	  • Erstellen einer Workstation-Audit-Map
	  • Bearbeiten einer Workstation-Audit-Map
	• CAC Software:
	  • Erstellen einer CAC-Audit-Map
	  • Bearbeiten einer CAC-Audit-Map

• SCIEX OS: Wenden Sie die Audit-Map auf den Workstation-Audit-Trail an. • CAC Software: Wenden Sie die Audit-Map auf den CAC-Audit-Trail an.	• SCIEX OS: Ändern einer aktiven Audit-Map für eine Workstation • CAC Software: Ändern einer aktiven Audit-Map für ein CAC-System
Erstellen einer standardmäßig aktiven Audit-Map für neue Projekte	• Erstellen einer Projekt-Audit-Map.
Konfiguration der Audit-Map, die für bestehende Projekte verwenden werden soll	• Erstellen einer Projekt-Audit-Map. • Bearbeiten einer Projekt-Audit-Map.
Anwendung der Audit-Map auf bestehende Projekte	• Ändern einer aktiven Audit-Map für ein Projekt.

Installierte Audit-Map-Vorlagen

Die Software umfasst mehrere Audit-Map-Vorlagen. Diese Vorlagen können nicht bearbeitet oder gelöscht werden.

Tabelle 7-3: Installierte Audit-Maps

Audit-Map	Beschreibung
Beispiel-Audit-Map	Ausgewählte Ereignisse werden geprüft. Nur zu Darstellungszwecken.
Vollständige Audit-Map	Alle Ereignisse werden geprüft. Für alle Ereignisse sind elektronische Signaturen und Gründe erforderlich.
Keine Audit-Map	Es werden keine Ereignisse überprüft. **Hinweis:** Das Ereignis **Zuweisung der aktiven Audit-Map ändern** wird immer aufgezeichnet, auch wenn die Vorlage „No Audit Map“ verwendet wird.
Im Hintergrund arbeitende Audit-Map	Alle Ereignisse werden geprüft. Für keines der Ereignisse werden elektronische Signaturen und Gründe verlangt.

Für Beschreibungen der Audit-Trail-Arten und ihrer Beziehungen zu Audit-Maps siehe die Tabelle: Tabelle 7-1. Für Informationen über die in Audit-Trails erfassten Ereignisse siehe Abschnitt: SCIEX OS-Audit-Trail-Aufzeichnungen.

Für Informationen über den Prüfprozess siehe die Tabelle: Tabelle 7-2.

Arbeiten mit Audit-Maps

Die Software umfasst mehrere installierte Audit-Map-Vorlagen. Für Beschreibungen der Audit-Map-Vorlagen siehe Abschnitt: Installierte Audit-Map-Vorlagen. Für eine Checkliste der empfohlenen Schritte beim Einrichten von Audits siehe Abschnitt: Einrichten von Audit-Maps.

Wenn eine aktive Audit-Map-Vorlage in der Software oder im Datei-Explorer gelöscht wird, dann verwendet ein Projekt, das diese Audit-Map-Vorlage verwendet, stattdessen die Silent-Audit-Map.

Projekt-Audit-Maps

Projekt-Audit-Maps steuern die Auditierung von Projektereignissen. Für eine Liste auditierbarer Projektereignisse siehe Abschnitt: Projekt-Audit-Trail.

Erstellen einer Projekt-Audit-Map

1. Öffnen Sie den Arbeitsbereich „Konfiguration“.
2. Klicken Sie auf **Audit-Maps**.
3. Öffnen Sie die Registerkarte Projektvorlagen.

4. Wählen Sie im Feld **Map-Vorlage bearbeiten** eine Vorlage als Grundlage für die neue Map aus.
5. Klicken Sie auf **Vorlage hinzufügen** ().
   Das Dialogfeld Projekt-Audit-Map-Vorlage hinzufügen wird geöffnet.
6. Geben Sie den Namen der neuen Map ein und klicken Sie dann auf **OK**.
7. Für die Auswahl und Konfiguration der aufzuzeichnenden Ereignisse gehen Sie wie folgt vor:
   a. Markieren Sie das Kontrollkästchen **Geprüft** für das Ereignis.
   b. (Optional) Wenn ein Grund erforderlich ist, wählen Sie **Grund erforderlich** aus.
   c. (Optional) Wenn eine elektronische Signatur erforderlich ist, wählen Sie **E-Sig. erforderlich** aus.
   d. (Optional) Wenn vordefinierte Gründe erforderlich sind, wählen Sie **Nur vordefinierten Grund verwenden** aus und definieren Sie die Gründe.
8. Achten Sie darauf, dass das Kontrollkästchen **Geprüft** für Ereignisse, die nicht protokolliert werden sollen, frei bleibt.
9. Klicken Sie auf **Vorlage speichern**.
   Das System fragt, ob die neue Map auf Projekte angewendet werden soll.
10. Führen Sie einen der folgenden Schritte aus:
    - Um die neue Map auf Projekte anzuwenden, klicken Sie auf **Ja**, wählen Sie die Projekte für die neue Map aus und klicken Sie dann auf **Anwenden**.
    - Wenn die neue Map nicht auf vorhandene Projekte angewendet werden soll, klicken Sie auf **Nein**.
11. (Optional) Klicken Sie auf **Als Standard für neue Projekte verwenden**, um diese Audit Map als Standard für alle neuen Projekte zu verwenden.

Bearbeiten einer Projekt-Audit-Map

Hinweis: Installierte Audit-Map-Vorlagen können nicht bearbeitet werden.

1. Öffnen Sie den Arbeitsbereich „Konfiguration“.
2. Klicken Sie auf **Audit-Maps**.
3. Öffnen Sie die Registerkarte Projektvorlagen.
4. Wählen Sie im Feld **Map-Vorlage bearbeiten** die zu ändernde Map aus.
5. Für die Auswahl und Konfiguration der aufzuzeichnenden Ereignisse gehen Sie wie folgt vor:
   a. Markieren Sie das Kontrollkästchen **Geprüft** für das Ereignis.
   b. (Optional) Wenn ein Grund erforderlich ist, wählen Sie **Grund erforderlich** aus.

c. (Optional) Wenn eine elektronische Signatur erforderlich ist, wählen Sie **E-Sig. erforderlich** aus.

d. (Optional) Wenn vordefinierte Gründe erforderlich sind, wählen Sie **Nur vordefinierten Grund verwenden** aus und definieren Sie die Gründe.

6. Achten Sie darauf, dass das Kontrollkästchen **Geprüft** für Ereignisse, die nicht protokolliert werden sollen, frei bleibt.
7. Klicken Sie auf **Vorlage speichern**.
   Das System fragt, ob die neue Map auf Projekte angewendet werden soll.
8. Führen Sie einen der folgenden Schritte aus:
   - Um die neue Map auf Projekte anzuwenden, klicken Sie auf **Ja**, wählen Sie die Projekte für die neue Map aus und klicken Sie dann auf **Anwenden**.
   - Wenn die neue Map nicht auf vorhandene Projekte angewendet werden soll, klicken Sie auf **Nein**.

Ändern einer aktiven Audit-Map für ein Projekt

Wenn eine Audit-Map für ein Projekt angewendet wird, ist sie eine aktive Audit-Map. Die Audit-Konfiguration in der aktiven Audit-Map bestimmt, welche Ereignisse in den Audit-Trails aufgezeichnet werden.

1. Öffnen Sie den Arbeitsbereich „Konfiguration“.
2. Klicken Sie auf **Audit-Maps**.
3. Öffnen Sie die Registerkarte „Projektvorlagen“.
4. Wählen Sie im Feld **Map-Vorlage bearbeiten** die Audit-Map aus, die dem Projekt zugewiesen werden soll.
5. Klicken Sie auf **Auf vorhandene Projekte anwenden**.
   Das Dialogfeld „Projekt-Audit-Map-Vorlage anwenden“ wird geöffnet.
6. Aktivieren Sie die Kontrollkästchen für die Projekte, auf die diese Audit-Map angewendet werden soll.
7. Klicken Sie auf **Anwenden**.

Löschen einer Projekt-Audit-Map

Hinweis: Installierte Audit-Map-Vorlagen können nicht gelöscht werden.

1. Öffnen Sie den Arbeitsbereich „Konfiguration“.
2. Klicken Sie auf **Audit-Maps**.
3. Öffnen Sie die Registerkarte Projektvorlagen.
4. Wählen Sie im Feld **Map-Vorlage bearbeiten** die zu löschende Map aus.
5. Klicken Sie auf **Vorlage löschen**.
   Das System fordert Sie zur Bestätigung auf.

6. Klicken Sie auf **Ja**.

Workstation-Audit-Maps

Workstation-Audit-Maps steuern die Auditierung von Workstation-Ereignissen. Für eine Liste auditierbarer Workstation-Ereignisse siehe Abschnitt: Workstation-Audit-Trail.

Erstellen einer Workstation-Audit-Map

1. Öffnen Sie den Arbeitsbereich „Konfiguration“.
2. Klicken Sie auf **Audit-Maps**.
3. Öffnen Sie die Registerkarte „Workstation-Vorlagen“.
4. Wählen Sie im Feld **Map-Vorlage bearbeiten** eine Vorlage als Grundlage für die neue Map aus.
5. Klicken Sie auf **Vorlage hinzufügen** ().
   Das Dialogfeld „Audit-Map-Vorlage für Workstation hinzufügen“ wird geöffnet.
6. Geben Sie den Namen der neuen Map ein und klicken Sie dann auf **OK**.
7. Für die Auswahl und Konfiguration der aufzuzeichnenden Ereignisse gehen Sie wie folgt vor:
   a. Markieren Sie das Kontrollkästchen **Geprüft** für das Ereignis.
   b. (Optional) Wenn ein Grund erforderlich ist, wählen Sie **Grund erforderlich** aus.
   c. (Optional) Wenn eine elektronische Signatur erforderlich ist, wählen Sie **E-Sig. erforderlich** aus.
   d. (Optional) Wenn vordefinierte Gründe erforderlich sind, wählen Sie **Nur vordefinierten Grund verwenden** aus und definieren Sie die Gründe.
8. Achten Sie darauf, dass das Kontrollkästchen **Geprüft** für Ereignisse, die nicht protokolliert werden sollen, frei bleibt.
9. Klicken Sie auf **Vorlage speichern**.
10. (Optional) Klicken Sie auf **Auf die Workstation anwenden**, um die Audit-Map als aktive Audit-Map für die Workstation zu verwenden.

Bearbeiten einer Workstation-Audit-Map

Hinweis: Installierte Audit-Map-Vorlagen können nicht bearbeitet werden.

1. Öffnen Sie den Arbeitsbereich „Konfiguration“.
2. Klicken Sie auf **Audit-Maps**.
3. Öffnen Sie die Registerkarte „Workstation-Vorlagen“.
4. Wählen Sie im Feld **Map-Vorlage bearbeiten** die zu ändernde Map aus.

5. Für die Auswahl und Konfiguration der aufzuzeichnenden Ereignisse gehen Sie wie folgt vor:
   a. Markieren Sie das Kontrollkästchen **Geprüft** für das Ereignis.
   b. (Optional) Wenn ein Grund erforderlich ist, wählen Sie **Grund erforderlich** aus.
   c. (Optional) Wenn eine elektronische Signatur erforderlich ist, wählen Sie **E-Sig. erforderlich** aus.
   d. (Optional) Wenn vordefinierte Gründe erforderlich sind, wählen Sie **Nur vordefinierten Grund verwenden** aus und definieren Sie die Gründe.
6. Achten Sie darauf, dass das Kontrollkästchen **Geprüft** für Ereignisse, die nicht protokolliert werden sollen, frei bleibt.
7. Klicken Sie auf **Vorlage speichern**.
8. (Optional) Klicken Sie auf **Auf die Workstation anwenden**, um die Audit-Map als aktive Audit-Map für die Workstation zu verwenden.

Ändern einer aktiven Audit-Map für eine Workstation

Wenn eine Audit-Map für eine Workstation angewendet wird, ist sie eine aktive Audit-Map. Die Audit-Konfiguration in der aktiven Audit-Map bestimmt, welche Ereignisse in den Audit-Trails aufgezeichnet werden.

1. Öffnen Sie den Arbeitsbereich „Konfiguration“.
2. Klicken Sie auf **Audit-Maps**.
3. Öffnen Sie die Registerkarte „Workstation-Vorlagen“.
4. Wählen Sie im Feld **Map-Vorlage bearbeiten** die Map aus, die auf die Workstation angewendet werden soll.
5. Klicken Sie auf **Auf die Workstation anwenden**.

Löschen einer Workstation-Audit-Map

Hinweis: Installierte Audit-Map-Vorlagen können nicht gelöscht werden.

1. Öffnen Sie den Arbeitsbereich „Konfiguration“.
2. Klicken Sie auf **Audit-Maps**.
3. Öffnen Sie die Registerkarte „Workstation-Vorlagen“.
4. Wählen Sie im Feld **Map-Vorlage bearbeiten** die zu löschende Map aus.
5. Klicken Sie auf **Vorlage löschen**.
   Das System fordert Sie zur Bestätigung auf.
6. Klicken Sie auf **Ja**.

CAC-Audit-Maps

CAC-Audit-Maps steuern die Auditierung von CAC-Workstation-Ereignissen. Eine Liste der auditierbaren Ereignisse finden Sie im Abschnitt: Workstation-Audit-Trail.

Erstellen einer CAC-Audit-Map

1. Öffnen Sie den Arbeitsbereich „Konfiguration“.
2. Klicken Sie auf **Audit-Maps**.
3. Öffnen Sie die Registerkarte „CAC-Vorlagen“.
4. Wählen Sie im Feld **Map-Vorlage bearbeiten** eine Vorlage als Grundlage für die neue Map aus.
5. Klicken Sie auf **Vorlage hinzufügen** ().
   Das Dialogfeld „CAC-Audit-Map-Vorlage hinzufügen“ wird geöffnet.
6. Geben Sie den Namen der neuen Map ein und klicken Sie dann auf **OK**.
7. Für die Auswahl und Konfiguration der aufzuzeichnenden Ereignisse gehen Sie wie folgt vor:
   a. Markieren Sie das Kontrollkästchen **Geprüft** für das Ereignis.
   b. (Optional) Wenn ein Grund erforderlich ist, wählen Sie **Grund erforderlich** aus.
   c. (Optional) Wenn eine elektronische Signatur erforderlich ist, wählen Sie **E-Sig. erforderlich** aus.
   d. (Optional) Wenn vordefinierte Gründe erforderlich sind, wählen Sie **Nur vordefinierten Grund verwenden** aus und definieren Sie die Gründe.
8. Achten Sie darauf, dass das Kontrollkästchen **Geprüft** für Ereignisse, die nicht protokolliert werden sollen, frei bleibt.
9. Klicken Sie auf **Vorlage speichern**.
10. (Optional) Um diese Audit-Map als aktive Audit-Map für die CAC-Workstation zu verwenden, klicken Sie auf **Auf die CAC anwenden**.

Bearbeiten einer CAC-Audit-Map

Hinweis: Installierte Audit-Map-Vorlagen können nicht bearbeitet werden.

1. Öffnen Sie den Arbeitsbereich „Konfiguration“.
2. Klicken Sie auf **Audit-Maps**.
3. Öffnen Sie die Registerkarte „CAC-Vorlagen“.
4. Wählen Sie im Feld **Map-Vorlage bearbeiten** die zu ändernde Map aus.
5. Für die Auswahl und Konfiguration der aufzuzeichnenden Ereignisse gehen Sie wie folgt vor:

a. Markieren Sie das Kontrollkästchen **Geprüft** für das Ereignis.

b. (Optional) Wenn ein Grund erforderlich ist, wählen Sie **Grund erforderlich** aus.

c. (Optional) Wenn eine elektronische Signatur erforderlich ist, wählen Sie **E-Sig. erforderlich** aus.

d. (Optional) Wenn vordefinierte Gründe erforderlich sind, wählen Sie **Nur vordefinierten Grund verwenden** aus und definieren Sie die Gründe.

6. Achten Sie darauf, dass das Kontrollkästchen **Geprüft** für Ereignisse, die nicht protokolliert werden sollen, frei bleibt.
7. Klicken Sie auf **Vorlage speichern**.
8. (Optional) Um diese Audit-Map als aktive Audit-Map für die CAC-Workstation zu verwenden, klicken Sie auf **Auf die CAC anwenden**.

Ändern einer aktiven Audit-Map für ein CAC-System

Wenn eine Audit-Map auf die CAC-Workstation angewendet wird, ist sie eine aktive Audit-Map. Die Audit-Konfiguration in der aktiven Audit-Map bestimmt, welche Ereignisse in den Audit-Trails aufgezeichnet werden.

1. Öffnen Sie den Arbeitsbereich „Konfiguration“.
2. Klicken Sie auf **Audit-Maps**.
3. Öffnen Sie die Registerkarte „CAC-Vorlagen“.
4. Wählen Sie im Feld **Map-Vorlage bearbeiten** die Map aus, die auf die CAC-Workstation angewendet werden soll.
5. Klicken Sie auf **Auf die CAC anwenden**.

Löschen einer CAC-Audit-Map

Hinweis: Installierte Audit-Map-Vorlagen können nicht gelöscht werden.

1. Öffnen Sie den Arbeitsbereich „Konfiguration“.
2. Klicken Sie auf **Audit-Maps**.
3. Öffnen Sie die Registerkarte „CAC-Vorlagen“.
4. Wählen Sie im Feld **Map-Vorlage bearbeiten** die zu löschende Map aus.
5. Klicken Sie auf **Vorlage löschen**.
   Das System fordert Sie zur Bestätigung auf.
6. Klicken Sie auf **Ja**.

Anzeigen, Durchsuchen, Exportieren und Drucken von Audit Trails

Dieser Abschnitt enthält Informationen über das Anzeigen von Audit Trails und archivierten Audit Trails. Er enthält auch Anweisungen zum Exportieren, Drucken, Durchsuchen und Sortieren von Audit-Aufzeichnungen innerhalb von Audit Trails.

Anzeigen von Audit-Trail-Aufzeichnungen

1. Öffnen Sie den Arbeitsbereich „Audit-Trail“.
2. Klicken Sie im linken Teilfenster auf den Audit-Trail, der angezeigt werden soll.
3. Um detaillierte Informationen zu einem Audit-Ereignis anzuzeigen, klicken Sie auf das Ereignis.

   Der ausgewählte Ereignistyp steuert die angezeigten Informationen. Die Informationen werden auf einer oder mehreren der folgenden Registerkarten angezeigt.

Tabelle 7-4: Registerkarten „Event Detail“

Registerkarte	Informationen
Allgemeine Details	Zeigt Informationen wie den Zeitzonenversatz und den Workstation-Namen an.
Vor der Änderung	Zeigt den Inhalt vor der vorgenommenen Änderung an.
Nach der Änderung	Zeigt den Inhalt nach der vorgenommenen Änderung an.
Änderungsdetails	Zeigt den ursprünglichen Inhalt und den neuen Inhalt im selben Teilfenster an. In der Differenz-Ansicht wird der ursprüngliche Inhalt rot dargestellt und der neue Inhalt wird grün dargestellt. In der Ansicht nebeneinander werden der ursprüngliche und der neue Inhalt in verschiedenen Teilfenstern angezeigt, sodass der Benutzer die Änderungen leicht erkennen kann.

Durchsuchen oder Filtern von Audit-Aufzeichnungen

1. Öffnen Sie den Arbeitsbereich „Audit-Trail“.
2. Wählen Sie den zu durchsuchenden Audit-Trail aus.
3. Um nach bestimmten Auditdatensätzen zu suchen, geben Sie Text in das Feld **Auf Seite suchen** ein.
   Alle Suchergebnisse für den eingegebenen Text auf der Seite werden hervorgehoben.
4. Um die Audit-Trail-Aufzeichnungen zu filtern, gehen Sie wie folgt vor:
   a. Klicken Sie auf das Filter-Symbol (Trichter).
      Das Dialogfeld „Audit-Trail filtern“ wird geöffnet.

b. Geben Sie die Filterkriterien ein.

c. Klicken Sie auf **OK**.

Anzeigen eines archivierten Audit-Trails

Sobald ein Audit-Trail 20.000 Audit-Aufzeichnungen enthält, archiviert die SCIEX OS Software diese Aufzeichnungen automatisch und beginnt einen neuen Audit-Trail. Die Audit-Trail-Dateien werden unter einem Namen archiviert, der den Typ des Audit-Trails und das Datum und die Uhrzeit angibt. Der Dateiname für ein Workstation-Audit-Trail-Archiv hat zum Beispiel das Format `WorkstationAuditTrailData-<workstation name>>-<YYYY><MMDDHHMMSS>.atds`.

Dieses Verfahren kann auch verwendet werden, um einen Audit-Trail für eine Ergebnistabelle zu öffnen.

1. Öffnen Sie den Arbeitsbereich „Audit-Trail“.
2. Klicken Sie auf **Durchsuchen**.
3. Navigieren Sie zu dem zu öffnenden archivierten Audit-Trail, wählen Sie ihn aus und klicken Sie dann auf **OK**.

Hinweis: Um den Audit-Trail für eine Ergebnistabelle zu öffnen, wählen Sie die zugehörige `qsession`-Datei aus.

Drucken eines Audit-Trails

1. Öffnen Sie den Arbeitsbereich „Audit-Trail“.
2. Wählen Sie den zu druckenden Audit-Trail aus.
3. Klicken Sie auf **Drucken**.
   Das Dialogfeld „Drucken“ wird geöffnet.
4. Wählen Sie den Drucker aus und klicken Sie dann auf **OK**.

Exportieren von Audit-Trail-Aufzeichnungen

1. Öffnen Sie den Arbeitsbereich „Audit-Trail“.
2. Wählen Sie den zu exportierenden Audit-Trail aus.
3. Klicken Sie auf **Exportieren**.
4. Navigieren Sie zu dem Speicherort der exportierten Datei, geben Sie einen **Dateiname** ein und klicken Sie auf **Speichern**.
   Der Audit-Trail wird als CSV-Datei gespeichert.

SCIEX OS-Audit-Trail-Aufzeichnungen

Dieser Abschnitt beschreibt die Felder in den Audit-Trail-Aufzeichnungen.

Bei den Workstation- und Projekt-Audit-Trails handelt es sich um verschlüsselte Dateien.

Hinweis: Workstation-Audit-Trails und Archive werden im Ordner `Program Data\SCIEX\Audit Data` gespeichert. Projekt-Audit-Trails und Archive werden im Ordner `Audit Data` für das Projekt gespeichert.

Tabelle 7-5: Prüfdatensatz – Felder

Bezeichnung	Beschreibung
Zeitstempel	Das Datum und die Uhrzeit der Aufzeichnung des Datensatzes.
Ereignisname	Der Name des Ereignisses.
Beschreibung	Eine Beschreibung des Ereignisses.
Grund	Der Grund für das Ereignis.
E-Signatur	Gibt an, ob eine E-Signatur für das Ereignis eingegeben wurde.
Vollständiger Benutzername	Der Name des Benutzers. **Hinweis:** Bei Ereignissen, die durch eine Entscheidungsregel ausgelöst wurden, ist dies der Benutzer, der den Batch übergeben hat.
Benutzer	Die Benutzer-ID des Benutzers, der das Ereignis initiiert hat, das zur Erstellung des Datensatzes führte.
Kategorie	Die Funktion oder Kategorie, zu der das Ereignis gehört.

Das untere Teilfenster des Arbeitsbereichs „Audit-Trail“ zeigt detaillierte Informationen über ein ausgewähltes Ereignis, einschließlich Details zu eventuellen Änderungen.

Für Listen aller Ereignisse, die in den Workstation- und Projekt-Audit-Trails aufgezeichnet werden, siehe die Abschnitte: Workstation-Audit-Trail und Projekt-Audit-Trail.

CAC-Audit-Trail-Aufzeichnungen

Dieser Abschnitt beschreibt die Felder in den Audit-Trail-Aufzeichnungen.

Bei den CAC- und Projekt-Audit-Trails handelt es sich um verschlüsselte Dateien.

Hinweis: Die CAC-Audit-Trails und Archive werden im Ordner `Program Data\SCIEX\Audit Data` gespeichert. Projekt-Audit-Trails und Archive werden im Ordner `Audit Data` für das Projekt gespeichert.

Tabelle 7-6: Prüfdatensatz – Felder

Bezeichnung	Beschreibung
Zeitstempel	Das Datum und die Uhrzeit der Aufzeichnung des Datensatzes.
Ereignisname	Der Name des Ereignisses.
Beschreibung	Eine Beschreibung des Ereignisses.

Tabelle 7-6: Prüfdatensatz – Felder (Fortsetzung)

Bezeichnung	Beschreibung
Grund	Der Grund für das Ereignis.
E-Signatur	Gibt an, ob eine E-Signatur für das Ereignis eingegeben wurde.
Vollständiger Benutzername	Der Name des Benutzers. **Hinweis:** Bei Ereignissen, die durch eine Entscheidungsregel ausgelöst wurden, ist dies der Benutzer, der den Batch übergeben hat.
Benutzer	Die Benutzer-ID des Benutzers, der das Ereignis initiiert hat, das zur Erstellung des Datensatzes führte.
Kategorie	Die Funktion oder Kategorie, zu der das Ereignis gehört.

Das untere Teilfenster des Arbeitsbereichs „Audit-Trail“ zeigt detaillierte Informationen über ein ausgewähltes Ereignis, einschließlich Details zu eventuellen Änderungen.

Für Listen aller Ereignisse, die in den CAC- und Projekt-Audit-Trails aufgezeichnet werden, siehe die Abschnitte: Tabelle 3 und Projekt-Audit-Trail.

Audit-Trail-Archive

Audit-Aufzeichnungen sammeln sich im Projekt-Audit-Trail und im Workstation-Audit-Trail an. Die resultierenden Dateien können sehr groß werden und daher schwierig zu navigieren und zu verwalten sein.

Wenn ein Audit-Trail 20.000 Aufzeichnungen erreicht, wird er archiviert. Dem Audit-Trail wird eine letzte Archivaufzeichnung hinzugefügt. Sie wird unter einem Namen bestehend aus der Art des Audit-Trails, dem Datum und der Uhrzeit gespeichert. Es wird ein neuer Audit-Trail erstellt. Die erste Aufzeichnung im neuen Audit-Trail gibt an, dass der Audit-Trail archiviert wurde. Ebenfalls enthalten ist der Pfad zu dem archivierten Audit-Trail.

Workstation-Audit-Trail-Archive werden im Ordner `C:\ProgramData\SCIEX\Audit Data` gespeichert. Die Dateinamen sind im Format WorkstationAuditTrailData-<*Workstation-Name*>-<*JJJJ*><*MMTTHHMMSS*>.atds. Beispiel: `WorkstationAuditTrailData-SWDSXPT158-20190101130401.atds`.

Archive für Projekt-Audit-Trails werden im Ordner `Audit Data` für das Projekt gespeichert.

Zugriff auf Daten während Netzwerkunterbrechungen A

Lokale Anzeige und Prozessierung von Daten

Wenn während einer Netzwerkerfassung eine vorübergehende Netzwerkunterbrechung auftritt, können Sie auf dem Erfassungscomputer über den Ordner `NetworkBackup` auf die erfassten Daten zugreifen. Um die Beschädigung der Daten zu vermeiden, empfehlen wir dringend, die Datendateien aus dem `NetworkBackup`-Ordner an einen neuen Speicherort zu kopieren, bevor diese angezeigt oder verarbeitet werden. Die ursprünglichen Dateien sollten im Ordner `NetworkBackup` verbleiben.

Die SCIEX OS Software überprüft alle 15 Minuten, ob der Speicherplatz im Netzwerk verfügbar ist. Wenn dies der Fall ist, wird der Datentransfer fortgesetzt.

Der Ordner `NetworkBackup` wird in der Regel im lokalen Stammverzeichnis `D:\SCIEX OS Data\NetworkBackup` gespeichert. Die Datendateien für die einzelnen Batches werden in einem Ordner gespeichert, der mit einer eindeutigen Kennzeichnung benannt ist. Der Datums- und Zeitstempel der Ordner gibt das Startdatum und die Startzeit des Batchs an und kann Aufschluss darüber geben, welcher Ordner die gesuchten Daten enthält.

Entfernen von Proben aus einem Netzwerktransfer-Ordner

Wenn die Netzwerkverbindung für längere Zeit unterbrochen wird oder wenn das Stammverzeichnis des Netzwerks geändert wird, ist es möglicherweise erforderlich, Datendateien aus dem Ordner für den Netzwerktransfer zu entfernen. Wir empfehlen, diese Aktion von einem erfahrenen Systemadministrator mit fundierten technischen Netzwerkkenntnissen durchführen zu lassen.

1. Öffnen Sie den Arbeitsbereich „Warteschlange“.
2. Stoppen Sie die Warteschlange.
3. Brechen Sie alle verbleibenden Proben in dem Batch ab, der die zu entfernenden Proben enthält.
4. Schließen Sie die SCIEX OS Software.
5. Stoppen Sie **Clearcore2.Service.exe**.

   Tipp! Führen Sie diese Aufgabe im Windows Service Manager aus.

6. Verschieben Sie alle Dateien und Ordner in den Ordnern `OutBox` und `NetworkBackup`, die auf den Transfer in das nicht verfügbare Stammverzeichnis warten, vorübergehend in einen anderen Ordner. Löschen Sie nicht die Ordner `OutBox` oder `NetworkBackup`.

Hinweis: Der Ordner `OutBox` ist ein verborgener Ordner, der sich in der Regel im lokalen Stammverzeichnis `D:\SCIEX OS Data\TempData\Outbox` befindet. Wenn die Dateien und Ordner in `Outbox` nicht mehr benötigt werden, können Sie entfernt werden.

VORSICHT: Möglicher Datenverlust. Löschen Sie die Datei nicht, wenn die Daten der festsitzenden Probe erhalten bleiben müssen.

7. Öffnen Sie die SCIEX OS Software.
   Innerhalb von 15 Minuten versucht die SCIEX OS Software, eine Verbindung zur Netzwerkressource herzustellen. Wenn die Verbindung erfolgreich ist, wird der Transfer fortgesetzt. Wenn der Transfer abgeschlossen ist, werden die Ordner aus dem Ordner `NetworkBackup` gelöscht.

Windows-Berechtigungen B

Dieser Abschnitt enthält eine Liste der Windows-Berechtigungen, die für jede Benutzerrolle und für den SYSTEM-Benutzer für einen ordnungsgemäßen Betrieb der SCIEX OS Software erforderlich sind.

Hinweis: Der Standard-Pfad für den *Ordner „Installed Root Directory“* ist `D:\SCIEX OS Data`.

Tabelle B-1: *Ordner* „Installed Root Directory“

Berechtigung	Administrator, SYSTEM	Analyst, Methodenentwickler, Prüfer
Vollzugriff	Zulassen	—
Ordner durchsuchen / Datei ausführen	Zulassen	Zulassen
Ordner auflisten / Daten lesen	Zulassen	Zulassen
Attribute lesen	Zulassen	Zulassen
Erweiterte Attribute lesen	Zulassen	Zulassen
Dateien erstellen / Daten schreiben	Zulassen	Zulassen
Ordner erstellen / Daten anhängen	Zulassen	Zulassen
Attribute schreiben	Zulassen	Zulassen
Erweiterte Attribute schreiben	Zulassen	Zulassen
Unterordner und Dateien löschen	Zulassen	—
Löschen	Zulassen	—
Berechtigungen lesen	Zulassen	Zulassen

Tabelle B-1: *Ordner* „Installed Root Directory“ (Fortsetzung)

Berechtigung	Administrator, SYSTEM	Analyst, Methodenentwickler, Prüfer
Berechtigungen ändern	Zulassen	—
Besitz übernehmen	Zulassen	—

Tabelle B-2: Ordner *`Installed Root Directory`*`\NetworkBackup` und *`Installed Root Directory`*`\TempData`

Berechtigung	Administrator, SYSTEM	Analyst, Methodenentwickler, Prüfer
Vollzugriff	Zulassen	—
Ordner durchsuchen / Datei ausführen	Zulassen	Zulassen
Ordner auflisten / Daten lesen	Zulassen	Zulassen
Attribute lesen	Zulassen	Zulassen
Erweiterte Attribute lesen	Zulassen	Zulassen
Dateien erstellen / Daten schreiben	Zulassen	Zulassen
Ordner erstellen / Daten anhängen	Zulassen	Zulassen
Attribute schreiben	Zulassen	Zulassen
Erweiterte Attribute schreiben	Zulassen	Zulassen
Unterordner und Dateien löschen	Zulassen	Zulassen
Löschen	Zulassen	Zulassen
Berechtigungen lesen	Zulassen	Zulassen

Tabelle B-2: Ordner *Installed Root Directory*\NetworkBackup und *Installed Root Directory*\TempData (Fortsetzung)

Berechtigung	Administrator, SYSTEM	Analyst, Methodenentwickler, Prüfer
Berechtigungen ändern	Zulassen	—
Besitz übernehmen	Zulassen	—

Tabelle B-3: Ordner C:\ProgramData\SCIEX\Audit Data

Berechtigung	Administrator, SYSTEM	Analyst, Methodenentwickler, Prüfer
Vollzugriff	Zulassen	—
Ordner durchsuchen / Datei ausführen	Zulassen	Zulassen
Ordner auflisten / Daten lesen	Zulassen	Zulassen
Attribute lesen	Zulassen	Zulassen
Erweiterte Attribute lesen	Zulassen	Zulassen
Dateien erstellen / Daten schreiben	Zulassen	Zulassen
Ordner erstellen / Daten anhängen	Zulassen	Zulassen
Attribute schreiben	Zulassen	Zulassen
Erweiterte Attribute schreiben	Zulassen	Zulassen
Unterordner und Dateien löschen	Zulassen	—
Löschen	Zulassen	—
Berechtigungen lesen	Zulassen	Zulassen

Tabelle B-3: Ordner `C:\ProgramData\SCIEX\Audit Data` (Fortsetzung)

Berechtigung	Administrator, SYSTEM	Analyst, Methodenentwickler, Prüfer
Berechtigungen ändern	Zulassen	—
Besitz übernehmen	Zulassen	—

Audit-Ereignisse C

In diesem Abschnitt werden die Audit-Ereignisse in SCIEX OS aufgelistet. Es werden außerdem die entsprechenden Audit-Ereignisse in der Analyst Software aufgelistet für Benutzer, die eine Migration von der Analyst Software zu SCIEX OS durchführen.

Projekt-Audit-Trail

Jedes Projekt hat einen Projekt-Audit-Trail. Der Projekt-Audit-Trail wird im Ordner `Audit Data` für das Projekt gespeichert. Der Name der Audit-Trail-Datei ist „`ProjectAuditEvents.atds`“.

Hinweis: Die Standard-Audit-Map für neue Projekte, die in der Central Administrator Console (CAC) Software erstellt wurden, ist die Im Hintergrund arbeitende Audit-Map.

Ereignisse des Projekt-Audit-Trails werden sowohl in der CAC Software als auch in SCIEX OS angezeigt.

Tabelle C-1: Ereignisse des Projekt-Audit-Trails

SCIEX OS oder CAC	Analyst Software
Arbeitsbereich „Analyse“	
Ist-Konzentration wurde geändert	Quantifizierungsereignisse: **'Concentration' has been changed**
Datei für automatische Prozessierung wurde gespeichert	—
Barcode-ID wurde geändert	—
Vergleichsprobe wurde in nicht-zielgerichtetem Arbeitsablauf geändert	—
Benutzerdefinierte Spalten wurden geändert	Quantifizierungsereignisse: **'Custom Title' has changed**
Datenexploration wurde geöffnet	Projektereignisse: **Data File has been opened**
Daten wurden exportiert	—
Daten wurden an das LIMS übertragen	—
Verdünnungsfaktor wurde geändert	Quantifizierungsereignisse:: **'Dilution Factor' has been changed**
Externe Kalibrierung wurde geändert	—
Externe Kalibrierung wurde exportiert	—

Tabelle C-1: Ereignisse des Projekt-Audit-Trails (Fortsetzung)

SCIEX OS oder CAC	Analyst Software
Datei wurde gespeichert	Projektereignisse: **Quantitation Results Table has been created**, **Quantitation Results Table has been modified**, Quantifizierungsereignisse: **Results Table has been saved**
Formelspalte wurde geändert	Quantifizierungsereignisse:: **Formula name has been changed**, **Formula name has been added**, **Formula string has been changed**, **Formula column has been removed**
Integration wurde gelöscht	—
Integrationsparameter wurden geändert	Quantifizierungsereignisse: **Quantitation peak has been integrated**
Ergebnis der Bibliothekssuche wurde geändert	—
Manuelle Integration	Quantifizierungsereignisse: **Quantitation Peak has been integrated**
Manuelle Integration wurde rückgängig gemacht	Quantifizierungsereignisse: **Quantitation peak has been reverted back to original**
MS/MS-Auswahl wurde geändert	—
Prozessierungsmethode wurde geändert und angewendet	Quantifizierungsereignisse: **Quantitation method has been changed**
Prozessierungsmethode gespeichert	—
Die Standardeinstellungen des Projekts wurden geändert	—
Bericht wurde erstellt	Projektereignisse: **Printing document on printer, Finished printing document on printer**
Ergebnistabelle wurde genehmigt	Quantifizierungsereignisse: **QA reviewer has accessed a results table**
Ergebnistabelle wurde erstellt	Quantifizierungsereignisse: **Results table has been created**
Ergebnistabelle wurde gesperrt	—
Ergebnistabelle wurde entsperrt	—
Proben-ID wurde geändert	Quantifizierungsereignisse: **'Sample ID' has been changed**

Tabelle C-1: Ereignisse des Projekt-Audit-Trails (Fortsetzung)

SCIEX OS oder CAC	Analyst Software
Probenname wurde geändert	Quantifizierungsereignisse: **'Sample Name' has been changed**
Probentyp wurde geändert	Quantifizierungsereignisse: **'Sample Type' has been changed**
Proben wurden hinzugefügt oder entfernt	Quantifizierungsereignisse: **Files have been added to Results Table**, **Files have been removed from Results Table**, **Samples have been added/removed**
Standardzugabe Ist-Konzentration wurde geändert	—
Auswahl der verwendeten Spalte wurde geändert	Quantifizierungsereignisse: **'Use IT' has been changed**
Gewicht/Volumen geändert	**'Weight to Volume Ratio' has been changed**
Fenster/Bereich wurde gedruckt	Projektereignisse: **Printing document on printer**, **Finished printing document on printer**
Seite „Audit-Map“	
Projekt-Audit-Map wurde geändert	Projektereignisse: **Project Settings have been changed**
Projekt-Audit-Trail wurde exportiert	—
Projekt-Audit-Trail wurde gedruckt	—
Arbeitsbereich „Batch“	
Batch-Informationen wurden aus LIMS/ Text importiert	—
Batch gespeichert	—
Batch zur Warteliste gesendet	Instrumentenereignisse: **Batch file submitted**
Drucken	Projektereignisse: **Printing Document on printer**, **Finished printing document on printer**
Arbeitsbereich „Explorer“[4]	
Probe(n) öffnen	Projektereignisse: **Data File has been opened**

[4] Explorer-Ereignisse werden im Projekt-Audit-Trail aufgezeichnet, wenn Benutzer Daten im aktiven Projekt verwenden.

Tabelle C-1: Ereignisse des Projekt-Audit-Trails (Fortsetzung)

SCIEX OS oder CAC	Analyst Software
Drucken	Projektereignisse: **Printing Document on printer**, **Finished printing document on printer**
Probe(n) neu kalibrieren	—
Neukalibrierung der Probe(n) gestartet	—
Arbeitsbereich „LC-Methode“	
LC-Methode gespeichert	—
Drucken	Projektereignisse: **Printing Document on printer**, **Finished printing document on printer**
Arbeitsbereich „MS-Methode“	
MS-Methode gespeichert	—
Drucken	Projektereignisse: **Printing Document on printer**, **Finished printing document on printer**
Arbeitsbereich „Warteschlange“	
Die Probenerfassung ist abgeschlossen	—
Probe bearbeitet	—
Probe beginnt mit Erfassung	—
Probe wurde übertragen	—

Workstation-Audit-Trail

Jede Workstation hat einen Workstation-Audit-Trail. Der Workstation-Audit-Trail wird im Ordner „`Program Data\SCIEX\Audit Data`“ gespeichert. Der Name der Audit-Trail-Datei besitzt das Format: `WorkstationAuditTrailData.atds`.

Hinweis: Die Standard-Audit-Map für neue Workstations in der Central Administrator Console (CAC) Software ist die **Im Hintergrund arbeitende Audit-Map**.

Ereignisse des Audit-Trails werden sowohl in der CAC Software als auch in SCIEX OS angezeigt.

Tabelle C-2: Ereignisse des Workstation-Audit-Trails

SCIEX OS	Analyst Software
Audit-Map	

Tabelle C-2: Ereignisse des Workstation-Audit-Trails (Fortsetzung)

SCIEX OS	Analyst Software
Workstation-Audit-Map wurde geändert	Instrumentenereignisse: **Instrument Settings have been changed**
Workstation-Audit-Trail wurde gedruckt	—
Workstation-Audit-Trail wurde exportiert	—
CAC	
Zentraladministration aktiviert/deaktiviert	—
Einstellungen der Zentraladministration wurden abgerufen/konnten nicht abgerufen werden	—
Datendatei-Prüfsumme	
.wiff-Datendatei-Prüfsumme wurde geändert	—
Arbeitsbereich „Explorer“[5]	
Probe(n) öffnen	Projektereignisse: **Data File has been opened**
Drucken	Projektereignisse: **Printing document on printer**, **Finished printing document on printer**
Probe(n) neu kalibrieren	—
Neukalibrierung der Probe(n) gestartet	—
Hardwarekonfiguration	
Geräte aktiviert	Instrumentenereignisse: **Hardware profile has been activated**
Geräte deaktiviert	Instrumentenereignisse: **Hardware profile has been deactivated**
Geräte-Tuning	
Automatisches MS Tuning Update	Instrumentenereignisse: **Tune parameter settings changed**
Firmware wurde geändert	—
MS Tuning-Änderungen	Instrumentenereignisse: **Tune parameter settings changed**

[5] Explorer-Ereignisse werden im Workstation-Audit-Trail aufgezeichnet, wenn Benutzer Daten außerhalb des aktiven Projekts verwenden.

Tabelle C-2: Ereignisse des Workstation-Audit-Trails (Fortsetzung)

SCIEX OS	Analyst Software
Verfahrensergebnisse in MS Tune drucken	Projektereignisse: **Printing Document on printer**, **Finished printing document on printer**
Arbeitsbereich „Warteschlange“	
Automatische Injektion aufgetreten	—
Automatische erneute Injektion aufgetreten	—
Batch wurde in die Warteschlange verschoben	Instrumentenereignisse: **Move Batch**
Druckwarteschlange	Projektereignisse: **Printing Document on printer**, **Finished printing document on printer**
Probe neu erfassen	Instrumentenereignisse: **Reacquiring sample(s)**
Die Probenerfassung ist abgeschlossen	Projektereignisse: **Sample has been added to Data file**
Probe bearbeitet	—
Probe wurde in die Warteschlange verschoben	Instrumentenereignisse: **Sample moved from position *x* to position *y* of Batch File**
Probe beginnt mit Erfassung	—
Sicherheit	
Automatische Abmeldung durch das System	Instrumentenereignisse: **User Logged out**
Erzwungene Abmeldung durch einen anderen Benutzer	Instrumentenereignisse: **User Logged out**
Erzwungene Abmeldung fehlgeschlagen	—
Entsperren des Bildschirms fehlgeschlagen	—
Anmeldedaten des sicheren Netzwerkkontos (Secure Network Account, SNA) wurden geändert	Instrumentenereignisse: **Acquisition Account Changed**
Anmeldedaten des sicheren Netzwerkkontos (Secure Network Account, SNA) wurden entfernt	Instrumentenereignisse: **Acquisition Account Changed**

Tabelle C-2: Ereignisse des Workstation-Audit-Trails (Fortsetzung)

SCIEX OS	Analyst Software
Anmeldedaten des sicheren Netzwerkkontos (Secure Network Account, SNA) wurden spezifiziert	Instrumentenereignisse: **Acquisition Account Changed**
Sicherheitskonfiguration geändert	Instrumentenereignisse: **The Security Configuration has been modified**, **Screen Lock Changed**, **Auto Logout changed**
Benutzer wurde hinzugefügt/entfernt	Instrumentenereignisse: **User Added**, **User Deleted**
Benutzer hat sich angemeldet	Instrumentenereignisse: **User Logged In**
Benutzer hat sich abgemeldet	Instrumentenereignisse: **User Logged out**
Der Benutzer hat den exklusiven Modus ausgeschaltet	—
Benutzer-Anmeldung ist fehlgeschlagen	Instrumentenereignisse: **User Login Failed**
Einstellungen für die Benutzerverwaltung wurden exportiert	—
Einstellungen für die Benutzerverwaltung wurden importiert	—
Einstellungen für die Benutzerverwaltung wurden wiederhergestellt	—
Benutzerrolle wurde Benutzer/ Benutzergruppe zugewiesen	Instrumentenereignisse: **User Changed User Type**
Benutzerrolle wurde gelöscht	Instrumentenereignisse: **User Type Deleted**
Benutzerrolle wurde geändert	Instrumentenereignisse: **User Type Changed**
UserLog	
Ereignisprotokoll drucken	—

Tabelle C-3: CAC-Audit-Trail-Ereignisse

CAC	Analyst Software
Seite „Audit-Map“	
Workstation-Audit-Map wurde geändert	Instrumentenereignisse: **Instrument Settings have been changed**
Workstation-Audit-Trail wurde gedruckt	—
Workstation-Audit-Trail wurde exportiert	—

Tabelle C-3: CAC-Audit-Trail-Ereignisse (Fortsetzung)

CAC	Analyst Software
CAC	
CAC-Einstellungen wurden exportiert	—
CAC-Einstellungen wurden importiert	—
CAC-Einstellungen wurden wiederhergestellt	—
Projekteinstellungen in einer Arbeitsgruppe aktiviert/deaktiviert	—
Projekt zu einer Arbeitsgruppe zugewiesen bzw. die Zuweisung wurde aufgehoben	—
Sicherheitsberechtigung wurde für die Zentraladministration hinzugefügt	—
Benutzer wurde hinzugefügt/entfernt	—
Benutzerrolle wurde hinzugefügt	—
Benutzerrolle wurde gelöscht	—
Benutzerrolle wurde geändert	—
Benutzerrolle(n) wurde(n) Benutzer(n) in einer Arbeitsgruppe zugewiesen bzw. die Zuweisung wurde aufgehoben	—
Benutzer/Benutzergruppen wurden einer Arbeitsgruppe zugewiesen bzw. die Zuweisung wurde aufgehoben	—
Arbeitsgruppe wurde hinzugefügt/ gelöscht	—
Arbeitsgruppe wurde umbenannt	—
Workstation(s) wurde(n) einer Arbeitsgruppe zugewiesen bzw. die Zuweisung wurde aufgehoben	—
Sicherheit	
Automatische Abmeldung durch das System	Instrumentenereignisse: **User Logged out**
Erzwungene Abmeldung durch einen anderen Benutzer	Instrumentenereignisse: **User Logged out**
Erzwungene Abmeldung fehlgeschlagen	—

Tabelle C-3: CAC-Audit-Trail-Ereignisse (Fortsetzung)

CAC	Analyst Software
Entsperren des Bildschirms fehlgeschlagen	—
Anmeldedaten des sicheren Netzwerkkontos (Secure Network Account, SNA) wurden geändert	Instrumentenereignisse: **Acquisition Account Changed**
Anmeldedaten des sicheren Netzwerkkontos (Secure Network Account, SNA) wurden entfernt	Instrumentenereignisse: **Acquisition Account Changed**
Anmeldedaten des sicheren Netzwerkkontos (Secure Network Account, SNA) wurden spezifiziert	Instrumentenereignisse: **Acquisition Account Changed**
Sicherheitskonfiguration geändert	Instrumentenereignisse: **The Security Configuration has been modified**, **Screen Lock Changed**, **Auto Logout changed**
Benutzer wurde hinzugefügt/entfernt	Instrumentenereignisse: **User Added**, **User Deleted**
Benutzer hat sich angemeldet	Instrumentenereignisse: **User Logged In**
Benutzer hat sich abgemeldet	Instrumentenereignisse: **User Logged out**
Der Benutzer hat den exklusiven Modus ausgeschaltet	—
Benutzer-Anmeldung ist fehlgeschlagen	Instrumentenereignisse: **User Login Failed**
Einstellungen für die Benutzerverwaltung wurden exportiert	—
Einstellungen für die Benutzerverwaltung wurden importiert	—
Einstellungen für die Benutzerverwaltung wurden wiederhergestellt	—
Benutzerrolle wurde Benutzer/ Benutzergruppe zugewiesen	Instrumentenereignisse: **User Changed User Type**
Benutzerrolle wurde gelöscht	Instrumentenereignisse: **User Type Deleted**
Benutzerrolle wurde geändert	Instrumentenereignisse: **User Type Changed**
UserLog	
Ereignisprotokoll drucken	—

Zuordnung von Berechtigungen zwischen der SCIEX OS Software und der Analyst Software

D

Dieser Abschnitt ist für Benutzer, die eine Migration von der Analyst Software zur SCIEX OS Software durchführen, um ihnen dabei zu helfen, ihre Benutzersicherheitseinstellungen zu migrieren. Er zeigt die Berechtigungen in der Analyst Software, die den Berechtigungen in der SCIEX OS Software entsprechen.

Tabelle D-1: Zuordnung von Berechtigungen

SCIEX OS Software	Analyst Software
Arbeitsbereich „Batch“	
Entsperrte Methoden zur Warteliste senden	—
Öffnen	Batch: **Open Existing Batches**
Speichern unter	Batch: **Create New Batches**, **Import**, **Edit Batches**, **Save Batches**, **Overwrite Batches**
Zur Warteliste senden	Batch: **Submit Batches**
Speichern	Batch: **Save Batches**, **Overwrite Batches**
Ionenreferenztabelle speichern	—
Daten-Unterordner hinzufügen	—
Entscheidungsregeln konfigurieren	—
Arbeitsbereich „Konfiguration“	
Registerkarte „Allgemein“	—
Allgemein: Regionseinstellungen ändern	—
Allgemein: Vollbildmodus	—
Allgemein: Windows-Dienste stoppen	—
Registerkarte „LIMS-Kommunikation“	—
Registerkarte „Audit-Maps“	Audit Trail Manager: **Change Audit Trail Settings**, **Create or Modify Audit Maps**
Registerkarte „Warteschlange“	—
Warteschlange: Geräteleerlaufzeit	—

Tabelle D-1: Zuordnung von Berechtigungen (Fortsetzung)

SCIEX OS Software	Analyst Software
Warteschlange: Maximale Anzahl erfasster Proben	—
Warteschlange: Andere Warteschlangeneinstellungen	—
Registerkarte „Projekte“	—
Projekte: Projekt erstellen	Analyst-Anwendung: **Create Project**
Projekte: Eine Audit-Map-Vorlage auf ein bestehendes Projekt anwenden	Audit Trail Manager: **Change Audit Trail Settings**
Projekte: Stammverzeichnis erstellen	Analyst-Anwendung: **Create Root Directory**
Projekt: Aktuelles Stammverzeichnis festlegen	Analyst-Anwendung: **Set Root Directory**
Projekte: Netzwerkanmeldedaten festlegen	—
Projekte: Das Schreiben der Prüfsumme für die wiff-Datenerstellung aktivieren	—
Projekte: Stammverzeichnis löschen	—
Registerkarte „Geräte“	Hardwarekonfiguration: **Create**, **Delete**, **Edit**, **Activate/Deactivate**
Registerkarte „Benutzerverwaltung“	**Security Config**
Abmeldung des Benutzers erzwingen	**Unlock/Logout Application**
Registerkarte „CAC“[3]	—
Registerkarte „Druckvorlagen“	—
Druckvorlagen: Druckvorlagen erstellen und modifizieren	—
Druckvorlagen: Standard-Druckvorlage festlegen	—
Druckvorlagen: Die aktuelle Vorlage auf alle Projekte im Stammverzeichnis anwenden	
Arbeitsbereich „Ereignisprotokoll“	
Auf Arbeitsbereich „Ereignisprotokoll“ zugreifen	—

[3] In Version 3.1 wurde die Berechtigung **Zentraladministration aktivieren** umbenannt in **CAC**. Die Seite CAC im Arbeitsbereich „Konfiguration“ kann verwendet werden, um die Zentraladministration der SCIEX OS Software zu konfigurieren.

Tabelle D-1: Zuordnung von Berechtigungen (Fortsetzung)

SCIEX OS Software	Analyst Software
Protokoll archivieren	—
Arbeitsbereich „Audit-Trail“	
Auf Arbeitsbereich „Audit-Trail“ zugreifen	Audit Trail Manager: **View Audit Trail Data**
Aktive Audit-Map anzeigen	Audit Trail Manager: **View Audit Trail Data**
Audit-Trail drucken/exportieren	Audit Trail Manager: **View Audit Trail Data**
Feld „Data Acquisition“	
Start	—
Stopp	—
Speichern	—
Arbeitsbereiche „MS-Methode“ und „LC-Methode“	
Auf Arbeitsbereich „Methode“ zugreifen	—
Neu	Erfassungsmethode: **Create/Save acquisition method**
Öffnen	Erfassungsmethode: **Open acquisition method as read-only (acquire mode)**
Speichern	Erfassungsmethode: **Overwrite acquisition methods**, **Create/Save acquisition method**
Speichern unter	Erfassungsmethode: **Overwrite acquisition methods**, **Create/Save acquisition method**
Methode sperren/entsperren	—
Arbeitsbereich „Warteschlange“	
Verwalten	Proben-Warteschlange: **Reacquire**, **Delete Sample or Batch**, **Move Batch**
Start/Stopp	Proben-Warteschlange: **Start Sample**, **Stop Sample**, **Abort Sample**, **Stop Queue**
Drucken	Berichtsvorlagen-Editor: **Print**
Probe bearbeiten	—
Arbeitsbereich „Bibliothek“	

Tabelle D-1: Zuordnung von Berechtigungen (Fortsetzung)

SCIEX OS Software	Analyst Software
Auf Arbeitsbereich „Bibliothek“ zugreifen	Durchsuchen: **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**
Arbeitsbereich „MS Tune“	
Auf Arbeitsbereich „MS Tune“ zugreifen	—
Erweitertes MS-Tuning	Abstimmen: **Instrument Optimization**, **Manual Tune**, **Edit Tuning Options**
Erweiterte Fehlerbehebung	—
Schnelle Statusüberprüfung	Abstimmen: **Instrument Opt**
Instrumentendaten wiederherstellen	Abstimmen: **Edit Tuning Options**, **Edit instrument data**
Arbeitsbereich „Explorer“	
Auf Arbeitsbereich „Explorer“ zugreifen	—
Exportieren	Durchsuchen: **Save data to text file**
Drucken	Berichtsvorlagen-Editor: **Print**
Optionen	—
Erneut kalibrieren	Abstimmen: **Calibrate from current spectrum**
Arbeitsbereich „Analyse“	
Neue Ergebnisse	Quantifizierung: **Create new results tables**
Prozessierungsmethode erstellen	Quantifizierung: **Create quantitation methods**
Prozessierungsmethode ändern	Quantifizierung: **Modify existing methods**
Export nicht gesperrter Ergebnistabelle und Erstellen eines Berichts aus dieser erlauben	—
Ergebnisse speichern für Automatisierungs-Batch	—
Integrationsalgorithmus der standardmäßigen Quantifizierungsmethode ändern	Quantifizierung: **Change default method options**

Tabelle D-1: Zuordnung von Berechtigungen (Fortsetzung)

SCIEX OS Software	Analyst Software
Integrationsparameter der standardmäßigen Quantifizierungsmethode ändern	Quantifizierung: **Change default method options**
Warnung bei geänderten Peaks eines Projekts aktivieren	—
Proben hinzufügen	Quantifizierung: **Add and Remove samples from results table**
Ausgewählte Proben entfernen	Quantifizierung: **Add and Remove samples from results table**
Externe Kalibrierung exportieren, importieren oder entfernen	—
Probenname ändern	Quantifizierung: **Modify sample name**
Probentyp ändern	Quantifizierung: **Modify Sample Type**
Proben-ID ändern	Quantifizierung: **Modify Sample ID**
Ist-Konzentration ändern	Quantifizierung: **Modify Analyte Concentration**
Verdünnungsfaktor ändern	Quantifizierung: **Modify Dilution Factor**
Kommentarfelder ändern	Quantifizierung: **Modify Sample Comment**
Manuelle Integration aktivieren	Quantifizierung: **Manually integrate**
Peak auf „nicht gefunden“ setzen	—
Einen Peak in die Ergebnistabelle einbeziehen oder aus dieser ausschließen	Quantifizierung: **Exclude standards from calibration**
Regressionsoptionen	Quantifizierung: **Change regression parameters**
Integrationsparameter der Ergebnistabelle für ein einzelnes Chromatogramm ändern	Quantifizierung: **Change "simple" parameters in peak review**, **Change "advanced" parameters in peak review**
Quantifizierungsmethode für Komponente der Ergebnistabelle modifizieren	Quantifizierung: **Edit results tables’ method**
Neue Einstellungen für metrische Darstellungen erstellen	Quantifizierung: **Modify or create metric plot settings**
Benutzerdefinierte Spalten hinzufügen	Quantifizierung: **Create or modify formula columns**

Tabelle D-1: Zuordnung von Berechtigungen (Fortsetzung)

SCIEX OS Software	Analyst Software
Titelformat für die Peak-Überprüfung festlegen	—
Benutzerdefinierte Spalte entfernen	Quantifizierung: **Create or modify formula columns**
Einstellungen für die Anzeige der Ergebnistabelle	Quantifizierung: **Change results table column precision**, **Change results table column visibility**, **Modify results table settings**
Ergebnistabelle sperren	—
Ergebnistabelle entsperren	—
Ergebnisdatei als „geprüft“ kennzeichnen und speichern	—
Berichtsvorlage ändern	Berichtsvorlagen-Editor: **Create/Modify report templates**
Ergebnisse an LIMS übertragen	—
Barcode-Spalte ändern	—
Zuweisung der Vergleichsprobe ändern	—
MSMS-Spektren zur Bibliothek hinzufügen	Durchsuchen: **Add spectrum to library record**
Standardeinstellungen des Projekts	Quantifizierung: **Modify global (default) settings**
Bericht in allen Formaten erstellen	—
Parameter für die Markierungskriterien bearbeiten	—
Parameter für das automatische Entfernen von Ausreißern ändern	—
Automatische Entfernung von Ausreißern aktivieren	—
Prozessierungsmethode über FF/LS aktualisieren	—
Ergebnisse über FF/LS aktualisieren	—
Funktion der Gruppierung nach Addukten aktivieren	Quantifizierung: **Create Analyte Groups**, **Modify Analyte Groups**
Dateien suchen	—
Standardzugabe aktivieren	—

Tabelle D-1: Zuordnung von Berechtigungen (Fortsetzung)

SCIEX OS Software	Analyst Software
Prozentsatzregel für die manuelle Integration festlegen	Quantifizierung: **Enable or Disable percent rule in Manual Integration**
Gewicht/Volumen ändern	Quantifizierung: **Modify Weight To Volume ratio**

Datendatei-Prüfsumme E

Wir empfehlen den Nutzern, Datendatei-Prüfsummen für wiff-Dateien zu verwenden. Die Prüfsummenfunktion ist eine zyklische Redundanzprüfung, mit der die Integrität der Datendatei überprüft wird.

Wenn die „Data File Checksum“-Funktion aktiviert ist und eine Datendatei (wiff) erstellt wird, generiert die Software einen Prüfsummenwert mithilfe eines Algorithmus, der auf dem öffentlichen MD5-Verschlüsselungsalgorithmus basiert und speichert den Wert in der Datei. Wenn die Prüfsumme verifiziert wird, berechnet die Software die Prüfsumme und vergleicht die berechnete Prüfsumme mit der in der Datei gespeicherten Prüfsumme.

Der Prüfsummenvergleich kann zu drei Ergebnissen führen:

- Wenn die Werte übereinstimmen, ist die Prüfsumme gültig.
- Wenn die Werte nicht übereinstimmen, ist die Prüfsumme ungültig. Eine ungültige Prüfsumme zeigt an, dass entweder die Datei außerhalb der Software verändert oder die Datei bei aktivierter Prüfsummenberechnung gespeichert wurde und sich die Prüfsumme von der ursprünglichen Prüfsumme unterscheidet.
- Wenn die Datei keinen gespeicherten Prüfsummenwert enthält, wird keine Prüfsumme gefunden. Eine Datei hat keinen gespeicherten Prüfsummenwert, weil die Datei mit deaktivierter „Data File Checksum“-Funktion gespeichert wurde.

Hinweis: Der Benutzer kann die Prüfsumme mithilfe der Analyst Software überprüfen. Siehe die Dokumentation für die Analyst-Software.

Aktivieren oder Deaktivieren der Funktion „Data File Checksum“

1. Öffnen Sie den Arbeitsbereich „Konfiguration“.
2. Klicken Sie auf **Projekte**.
3. Erweitern Sie ggf. **Sicherheit von Datendateien**.
4. Aktivieren Sie das Kontrollkästchen **Das Schreiben der Prüfsumme für die wiff-Datenerstellung aktivieren**, um die Funktion „Data File Checksum“ zu aktivieren. Um die Funktion zu deaktivieren, deaktivieren Sie das Kontrollkästchen.

Kontakt

Kundenschulung

- In Nordamerika: NA.CustomerTraining@sciex.com
- In Europa: Europe.CustomerTraining@sciex.com
- Die Kontaktinformationen für Länder außerhalb der EU und Nordamerikas finden Sie unter sciex.com/education.

Online-Lernzentrum

- SCIEX Now Learning Hub

SCIEX Support

SCIEX und seine Vertretungen beschäftigen weltweit einen Stab an ausgebildeten Servicekräften und technischen Spezialisten. Der Support kann Fragen zum System oder anderen auftretenden, technischen Problemen beantworten. Weitere Informationen finden Sie auf der SCIEX-Website unter sciex.com, oder kontaktieren Sie uns unter:

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

Cybersicherheit

Die aktuellsten Hinweise zur Cybersicherheit von SCIEX-Produkten finden Sie unter sciex.com/productsecurity.

Dokumentation

Diese Version des Dokuments ersetzt alle vorherigen Versionen.

Um dieses Dokument elektronisch anzuzeigen, ist Adobe Acrobat Reader erforderlich. Die neueste Version finden Sie unter https://get.adobe.com/reader.

Softwareproduktdokumentationen entnehmen Sie den Versionshinweisen oder dem mit der Software mitgelieferten Software-Installationshandbuch.

Informationen zur Hardware-Produktdokumentation finden Sie in der mit dem System oder der Komponente gelieferten Dokumentation.

Die neuesten Versionen der Dokumentationen sind auf der Website von SCIEX unter sciex.com/customer-documents verfügbar.

Kontakt

Hinweis: Wenn Sie eine kostenlose gedruckte Ausgabe dieses Dokuments wünschen, wenden Sie sich bitte an sciex.com/contact-us.