SCIEX
The Power of Precision

Analyst MD Software

Handbuch für Laborleiter

IVD-IDV-05-0252-DE-E

April 2022

Dieses Dokument wird Käufern eines SCIEX-Geräts für dessen Gebrauch zur Verfügung gestellt. Dieses Dokument ist urheberrechtlich geschützt und jegliche Vervielfältigung dieses Dokuments, im Ganzen oder in Teilen, ist strengstens untersagt, sofern keine schriftliche Genehmigung von SCIEX vorliegt.

Die in diesem Dokument beschriebene Software unterliegt einer Lizenzvereinbarung. Das Kopieren, Ändern oder Verbreiten der Software auf einem beliebigen Medium ist rechtswidrig, sofern dies nicht ausdrücklich durch die Lizenzvereinbarung genehmigt wird. Darüber hinaus kann es nach der Lizenzvereinbarung untersagt sein, die Software zu disassemblieren, zurückzuentwickeln oder zurückzuübersetzen. Es gelten die aufgeführten Garantien.

Teile dieses Dokuments können sich auf andere Hersteller und/oder deren Produkte beziehen, die wiederum Teile enthalten können, deren Namen als Marken eingetragen sind und/oder die Marken ihrer jeweiligen Inhaber darstellen. Jede Nennung solcher Marken dient ausschließlich der Bezeichnung von Produkten eines Herstellers, die von SCIEX für den Einbau in die eigenen Geräte bereitgestellt werden, und bedeutet nicht, dass eigene oder fremde Nutzungsrechte und/oder -lizenzen zur Verwendung derartiger Hersteller- und/oder Produktnamen als Marken vorliegen.

Die Garantien von SCIEX beschränken sich auf die zum Verkaufszeitpunkt oder bei Erteilung der Lizenz für die eigenen Produkte ausdrücklich zuerkannten Garantien und sind die von SCIEX alleinig und ausschließlich zuerkannten Zusicherungen, Garantien und Verpflichtungen. SCIEX gibt keinerlei andere ausdrückliche oder implizite Garantien wie beispielsweise Garantien zur Marktgängigkeit oder Eignung für einen bestimmten Zweck, unabhängig davon, ob diese auf gesetzlichen oder sonstigen Rechtsvorschriften beruhen oder aus Geschäftsbeziehungen oder Handelsbrauch entstehen, und lehnt alle derartigen Garantien ausdrücklich ab; zudem übernimmt SCIEX keine Verantwortung und Haftungsverhältnisse, einschließlich solche in Bezug auf indirekte oder nachfolgend entstehenden Schäden, die sich aus der Nutzung durch den Käufer oder daraus resultierende widrige Umstände ergeben.

IVD

CE

UK CA

Zur Verwendung in der *In-vitro*-Diagnostik. Das Produkt/die Produkte ist/sind nicht in allen Ländern verfügbar. Weitere Informationen erhalten Sie von Ihrem lokalen Vertriebspartner oder unter sciex.com/diagnostics.

Rx only.

Die hier erwähnten Marken und/oder eingetragenen Marken, einschließlich deren Logos, sind Eigentum der AB Sciex Pte. Ltd. oder ihrer jeweiligen Inhaber in den Vereinigten Staaten und/oder anderen Ländern (siehe sciex.com/trademarks).

AB Sciex™ wird unter Lizenz verwendet.

© 2022 DH Tech. Dev. Pte. Ltd.

EC REP

Leica Microsystems CMS GmbH
Ernst-Leitz-Strasse 17-37
35578 Wetzlar
Germany

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

Inhalt

Kapitel 1: Einleitung **7**

Kapitel 2: Übersicht über die Sicherheitskonfiguration **8**
Sicherheit und Einhaltung gesetzlicher Vorschriften 8
Sicherheitsanforderungen 8
Analyst MD-Software und Windows-Sicherheit: Zusammenarbeit 8
Audit-Trails innerhalb der Analyst MD-Software und Windows 9
Audit-Trails in der MultiQuant MD Software 9
21 CFR Teil 11 9
Systemkonfiguration 10
Windows-Sicherheitskonfiguration 10
Benutzer und Gruppen 10
Unterstützung von Active Directory 11
Windows-Dateisystem 11
System-Audits 11
Datei- und Ordnerberechtigungen 11
Ereignisprotokolle 12
Windows-Benachrichtigungen 12

Kapitel 3: Elektronische Lizenzierung **13**

Kapitel 4: Konfiguration der Analyst MD Software-Sicherheit **14**
Workflow für die Software-Sicherheit 14
Analyst MD-Softwareinstallation 16
Überprüfen von Softwarekomponenten 16

Kapitel 5: Analyst MD-Software-Sicherheitskonfiguration **18**
Schritte zur Konfiguration der Analyst MD Software 18
Speicherplatz der sicherheitsrelevanten Informationen 18
Über Sicherheitsmodi und Konten 19
Auswählen des Sicherheitsmodus 20
Ein Erfassungskonto auswählen 21
Einrichten von Bildschirmsperre und automatischem Abmelden 22
Entsperren oder Abmelden von der Analyst MD Software 23
Zugriff auf die Analyst MD-Software 24
Über Benutzer und Rollen 24
Analyst MD Software-Zugriff 27
MultiQuant MD Software-Zugriff 39
Einen Benutzer oder eine Gruppe in der Analyst MD Software hinzufügen 43
Ändern einer Rolle 43

Personen von der Analyst MD Software entfernen 44
Erstellen einer benutzerdefinierten Rolle 44
Löschen einer benutzerdefinierten Rolle 45
Zugriff festlegen 46
Konfiguration der Windows-Firewall auf dem Erfassungs- und dem Clientcomputer 49
Remote-Workstations 51
Drucken der Sicherheitskonfigurationen 56

Kapitel 6: Überwachung des Systemstatus 57
Zusätzliche Kurven 57
Zusätzliche Kurven aktivieren 57
Zusätzliche Kurven anzeigen 57
Injektionszähler 58
Den Injektionszähler aktivieren 58

Kapitel 7: Auditing 60
Audit-Trails 60
Audit-Maps 61
Einrichten von Audit-Maps 62
Installierte Audit-Maps 63
Arbeiten mit Audit-Maps 64
Erstellen einer Audit Map 64
Ändern einer Audit Map 66
Kopieren einer Audit Map aus einem anderen Projekt 66
Anwenden einer Audit Map 67
Anzeigen, Drucken und Durchsuchen von Audit Trails 68
Anzeigen eines Audit-Trails 68
In eine „Results Table“ eingebettete Audit-Konfiguration anzeigen 68
Anzeigen von Details einer Audit-Aufzeichnung im Instrument Audit Trail 69
Anzeigen eines archivierten Audit-Trails 69
Drucken eines Audit-Trails 70
Suchen nach einer Audit-Aufzeichnung 70

Anhang A: Audit-Trails 72
Audit-Trail-Aufzeichnungen 72
Audit-Trail-Archive 72
Ereignisse im Geräte-Audit-Trail 73
Ereignisse des Projekt-Audit-Trails 74
Ereignisse des Quantitation Audit Trail 75
AAC Audit-Trail 77

Anhang B: Zusätzliche Sicherheitsanpassungen 78
Dateiänderungen („Explore Processing“) 78
Erstellen von „Explore Processing History“-Dateien 79
Eine „Explore Processing History“-Datei anzeigen 79
Hinzufügen eines Eintrags in das Instrument-Wartungsprotokoll 79
Einen Eintrag des Instrument-Wartungsprotokolls anzeigen 80

Konfigurieren der E-Mail-Benachrichtigung 80
Datendatei-Prüfsumme 81
Überprüfen der Datendatei-Prüfsumme 82
Aktivieren oder Deaktivieren der Funktion „Data File Checksum“ 82

Anhang C: Besonderes Erfassungskonto 83

Kontaktangaben 84
Kundenschulung 84
Online-Lernzentrum 84
SCIEX Support 84
Cybersicherheit 84
Dokumentation 84

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 Analyst MD 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 Zugriffskontroll- und Auditing-Komponenten der Analyst MD-Software in Verbindung mit den Zugriffskontroll- und Auditing-Komponenten von Windows arbeiten. Außerdem wird die Konfiguration der Windows-Sicherheit vor der Installation der Analyst MD-Software beschrieben.

Sicherheit und Einhaltung gesetzlicher Vorschriften

Sicherheitsanforderungen

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

Analyst MD-Software und Windows-Sicherheit: Zusammenarbeit

Die Analyst MD 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 Analyst MD Software verfügt über drei Modi für den Systemzugriff mit ansteigender Sicherheit:

- „Single User“-Modus (Einzelnutzermodus)
- „Mixed Mode“ (Gemischter Modus)
- „Integrated Mode“ (Integrierter Modus) (Standardeinstellung)

Weitere Informationen über Sicherheitsmodi und Sicherheitseinstellungen finden Sie im Abschnitt: Über Sicherheitsmodi und Konten.

Darüber hinaus bietet die Analyst MD-Software vollständig konfigurierbare Rollen, die von den mit Windows verbundenen Benutzergruppen getrennt sind.Darüber hinaus bietet 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: Zugriff auf die Analyst MD-Software.

Audit-Trails innerhalb der Analyst MD-Software und Windows

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

Die Analyst MD Software bietet ein System von Audit-Trails, das die Anforderungen an elektronische Aufzeichnungen erfüllt. Separate Audit-Trail-Aufzeichnungen:

- Ergänzungen oder Austausch in Massenkalibrierungstabellen oder Auflösungstabellen, Änderungen der Systemkonfiguration, sicherheitsrelevante Ereignisse und Einträge im Geräte-Wartungsprotokoll.
- Erstellungs- und Änderungsereignisse für Projekte, Tuning, Chargen, Daten, Erfassungsmethoden, Quantifizierungsmethoden, „Results Tables“ und Berichtvorlagendateien sowie das Öffnen und Schließen von Modulen und Druckereignisse. Zu den Löschereignissen, die im Audit-Trail aufgezeichnet werden, gehören das Löschen von Geräten für den Remote-Viewer, das Löschen von Benutzern in der Analyst MD Software, das Löschen von Benutzertypen und das Löschen von Projektrollen.
- Erstellung und Änderung der in der „Results Table“ eingebetteten Quantifizierungsmethode, Änderung von Probeninformationen in der „Results Table“ und Änderung von Peak-Integrations-Parametern.

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

Die Analyst MD-Software verwendet Folgendes: Anwendungsereignisprotokoll, um Informationen über den Betrieb der Software zu erfassen. Verwenden Sie dieses Protokoll als Hilfe bei der Fehlerbehebung, weil Interaktionen von Massenspektrometer, Geräten und Software dort im Detail erfasst werden.

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.

Audit-Trails in der MultiQuant MD Software

DieMultiQuant MD Software enthält ihren eigenen Audit-Trail, der Erstellungs- und Änderungsereignisse innerhalb der MultiQuant MD Software prüft. Die „Audit Trail“-Funktion steht nur mit der „21 CFR Part 11“-Lizenz der MultiQuant MD Software zur Verfügung.

21 CFR Teil 11

Die Analyst MD-Software umfasst die technische Kontrolle zur Unterstützung von 21 CFR Teil 11 und implementiert dafür Folgendes:

- Verknüpfung der Sicherheit der Modi „Mixed“ (gemischt) und „Integrated“ (integriert) mit der Windows-Sicherheit
- Kontrollierter Zugriff auf Funktionen über anpassbare Rollen
- Kontrollierter, rollenbasierter oder gruppenbasierter Zugriff auf Projektdaten
- Audit-Trails für den Gerätebetrieb, die Wartung, 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 Analyst MD-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 Analyst MD-Software mit 21 CFR Teil 11 konform ist oder nicht, hängt von der tatsächlichen Nutzung und Konfiguration der Analyst MD-Software im Labor ab.

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

Systemkonfiguration

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

Windows-Sicherheitskonfiguration

Um die Analyst MD Software zum Verwalten Sicherheit verwenden zu können, muss der Administrator die Möglichkeit haben, Dateiberechtigungen für den Projektordner und alle zugehörigen Unterordner zu ändern. Wenn sich das Stammverzeichnis auf einem lokalen Computer befindet, könnte der Software-Administrator Teil der lokalen Administratoren-Gruppe sein. Nur der für das Sicherheitsmanagement verantwortliche Benutzer der Analyst MD-Software darf Mitglied der lokalen Administratorengruppe sein.

Damit die Analyst MD-Software wie vorgesehen funktioniert, müssen die Benutzer Mitglied der lokalen Microsoft Windows-Benutzergruppe sein.

Hinweis: Die Netzwerkerfassung wird von der Analyst MD-Software nicht unterstützt.

Benutzer und Gruppen

Die Analyst MD-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: Zugriff auf die Analyst MD-Software.

Unterstützung von Active Directory

„Active Directory“ kann entweder in „mixed“ (gemischten) oder „native“ (systemeigenen) Umgebungen arbeiten. Geben Sie im Sicherheitskonfigurationsfenster der Analyst MD-Software und in der Sicherheitsdatenbank der Analyst MD-Software Benutzerkonten im UPN-Format (User Principal Name) an.

Mixed Environment (Gemischte Umgebung)

Wenn die Analyst MD Software in einer gemischten Umgebung startet, dann enthält das Log-On-Fenster die Felder Benutzernamen, Kennwort und Domäne.

Das Netzwerk umfasst Folgendes:

- Windows-Server 2008 R2 und 2012.
- Windows 10, 64-Bit-Clients.

Native Environment (systemeigene Umgebung)

Wenn die Analyst MD Software in der nativen Umgebung startet, dann wird das Feld „Domain“ nicht angezeigt und die Analyst MD Software akzeptiert Benutzernamen ausschließlich im UPN-Format. Das Analyst MD Software Status-Fenster zeigt den Benutzernamen auch im UPN-Format.

Das Netzwerk umfasst Folgendes:

- Windows-Server 2008 R2 und 2012.
- Windows 10, 64-Bit-Clients.

Windows-Dateisystem

In der Analyst MD-Software müssen sich die Dateien und Verzeichnisse auf einer NTFS-formatierten Festplattenpartition befinden, die den Zugriff auf die Analyst MD-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.

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.

Datei- und Ordnerberechtigungen

Um die Sicherheit auf einem Netzlaufwerk zu verwalten, muss der Analyst MD Software-Administrator das Recht besitzen, Berechtigungen für den `Analyst Data`-Ordner und alle Unterordner zu ändern. Der Zugang muss durch den Netzwerkadministrator konfiguriert werden.

Vor der Auswahl der zu prüfenden Ereignisse oder Aktionen legen Sie die Berechtigungen für Dateien und Ordner fest. Die Berechtigungen für Ordner können auch für Unterordner und Dateien im Ordner gelten. Nachdem die Datei- und Ordnerberechtigungen eingerichtet wurden, definieren Sie die Ereignisse, die in das Sicherheitsprotokoll geschrieben werden.

Hinweis: Beziehen Sie dabei den Grad des Zugriffs, den die Benutzer auf das Laufwerk und den Ordner 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.

Weitere Informationen über die Datei- und Ordner-Berechtigungen der Analyst MD Software finden Sie im Abschnitt: Analyst MD-Software-Sicherheitskonfiguration.

Ereignisprotokolle

Öffnen Sie den Windows Event Viewer über die Analyst MD Software oder über Windows Administrative Tools. Der Windows Event Viewer zeichnet die überwachten Ereignisse im Sicherheits-, System- oder Anwendungsprotokoll auf.

Tipp! Um den Event Viewer von der Analyst MD Software aus zu öffnen klicken Sie auf **View** > **Event Log.**.

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 Messenger unter „Services“ (Dienste) 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

Die elektronische Lizenzierung kann ausschließlich knotenbasiert sein.

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 Analyst MD-Fenster auf **Help** > **About Analyst**.

Hinweis: Stellen Sie sicher, dass Sie die Lizenz verlängern, bevor sie abläuft.

Konfiguration der Analyst MD Software-Sicherheit 4

In diesem Abschnitt wird erläutert, wie man die Software konfiguriert.

Hinweis: Der Benutzer muss über lokale Administratorrechte für den Computer verfügen, auf dem die Software installiert wird.

Workflow für die Software-Sicherheit

Die Analyst MD 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.
- Zugriff auf die Analyst MD Software.
- Selektiver Zugriff auf die Analyst MD Software-Funktionalitäten.
- Zugriff auf bestimmte Projekte.
- Zugriff auf den Workstation-Status des Geräts

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: Workflow zum Konfigurieren der Sicherheit

Aufgabe	Verfahren
Installation der Analyst MD-Software.	Siehe das Dokument: *Analyst MD Software-Installationshandbuch*.
Konfiguration der Analyst MD-Software-Sicherheit.	Siehe Abschnitt: Analyst MD-Software-Sicherheitskonfiguration.
Konfiguration von Audit-Trails	Siehe Abschnitt: Auditing.
Konfiguration der Windows-Dateisicherheit und NTFS	Siehe Abschnitt: Zugriff festlegen.
Pflege des Systemwartungsprotokolls für Geräte, Sicherheit und Daten sowie Projektpflege	Siehe Abschnitt: Zusätzliche Sicherheitsanpassungen.

Tabelle 4-2: Optionen bei der Sicherheitskonfiguration

Option	CFR 21 Teil 11
Windows-Sicherheit	
Formatierung der Laufwerke als NTFS	Ja
Konfiguration von Benutzern und Gruppen	Ja
Aktivierung der Windows-Überwachung sowie der Datei- und Verzeichnisüberwachung	Ja
Einstellung von Dateiberechtigungen	Ja
Analyst MD Software-Installation	
Installation der Analyst MD-Software.	Ja
Installation der MultiQuant MD-Software	Ja
Auswahl von Audit-Optionen	Ja
Event Viewer (Installationsprüfung)	Ja
Analyst MD-Software-Sicherheit	
Auswahl des Sicherheitsmodus **Hinweis:** Die Verwendung des „Single User“-Modus (Einzelbenutzermodus) wird für die CFR-konforme Umgebung nicht empfohlen.	„Integrated“ (integriert) oder „Mixed“ (gemischt)
Konfiguration der Rollen und Personen für die Analyst MD Software.	Ja
Erstellen von Audit-Maps, Konfiguration von Audit-Trails für Geräte, Projekte und Quantifizierungen	Ja
Konfiguration von E-Mail-Benachrichtigungen	Ja
Prüfsummenaktivierung **Hinweis:** Die Prüfsummenfunktion wird standardmäßig bei der Neuinstallation der Analyst MD Software aktiviert.	Ja
Allgemeine Aufgaben	
Hinzufügen von neuen Projekten und Teilprojekten	Ja
Konfiguration eines Projekt-Audit-Trails für neue Projekte und Teilprojekte	Ja
Übertragung bestehender Daten	Ja
Erstellen eines Wartungsprotokolls für Gerätesicherheit, Daten und Projektpflege	Ja

Analyst MD-Softwareinstallation

Lesen Sie vor der Installation der Analyst MD 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.

Hinweis: Wir empfehlen, Windows-Updates und die Verbindung mit dem Internet für den Anwendungscomputer zu deaktivieren, um Änderungen an den Windows-Komponenten zu verhindern. Wenn die Updates und die Verbindung mit dem Internet nicht deaktiviert werden, muss das System nach Updates für Windows oder .NET Framework validiert werden. Für Erfassungscomputer wird dringend empfohlen, dass nur kritische Windows-Updates, wie beispielsweise Sicherheitsänderungen, installiert werden. Stellen Sie sicher, dass ein angemessener Virenschutz vorhanden ist, um eine Beeinträchtigung der Systemfunktion durch Viren zu verhindern.

Windows-Voraussetzungen

- Nur die englische Version des Betriebssystems Windows 10 wird unterstützt. Die Verwendung einer anderen Standardsprache kann dazu führen, dass die Software die Datei- oder Audit-Trail-Informationen falsch anzeigt.
- Achten Sie in den „Region and Language“-Einstellung darauf, dass **English (United States)** als erste Sprache eingestellt ist.

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-Maps. Nach der Installation kann der Administrator der Analyst MD-Software die Auswahl im „Security Configuration“-Modul ändern oder Audit-Maps im Audit Trail Manager konfigurieren.

Überprüfen von Softwarekomponenten

Nach der Installation der Analyst MD Software überprüft ein „Software Component Verification“-Verfahren, ob alle Software-Komponenten installiert wurden und erzeugt einen Installationsbericht. Dieser Bericht ist ein Ereignisprotokoll-Element aus dem Analyst MD Installer im Event Viewer Application-Protokoll. Überprüfen Sie unmittelbar nach Fertigstellung, ob die Installation erfolgreich war.

Es gibt ein Ereignisprotokoll für die Überprüfung der Prüfsumme der installierten Kern-Dateien. Weitere Informationen über die Prüfsumme finden Sie im Abschnitt: Datendatei-Prüfsumme.

1. Klicken Sie auf **Start** > **Control Panel.**

2. Doppelklicken Sie auf **Administrative Tools** und doppelklicken Sie dann auf **Event Viewer**.
3. Klicken Sie auf der Registerkarte **Tree** auf **Application Log**.
4. Klicken Sie auf das Ereignis **Analyst Installer**in der Spalte **Source**.
5. In der „Event Detail“-Nachricht gehen Sie im Feld **Description** auf **Total files verified**. Null Fehler sollten angezeigt werden.

Analyst MD-Software-Sicherheitskonfiguration 5

In diesem Abschnitt wird die Konfiguration der Analyst MD-Softwaresicherheit beschrieben.

Hinweis: Änderungen der Analyst MD-Software-Sicherheitskonfiguration werden nach dem Neustart der Analyst MD-Software wirksam.

Schritte zur Konfiguration der Analyst MD Software

Tipp! Stellen Sie beim Durchführen verschiedener Aufgaben im Dialogfeld „Security Configuration“ sicher, dass Sie auf den einzelnen Registerkarten auf **Apply** klicken, um die Änderungen zu speichern, bevor Sie zu einer anderen Registerkarte wechseln.

Informationen über die allgemeinen Aufgaben für die Konfiguration der Analyst MD Software finden Sie in der Tabelle: Tabelle 5-1

Tabelle 5-1: Aufgaben für die Konfiguration der Analyst MD Software

Aufgabe	Siehe
Konfigurieren des Sicherheitsmodus	Auswählen des Sicherheitsmodus.
Konfigurieren von Bildschirmsperre und automatischem Abmelden (nur Mixed-Modus)	Einrichten von Bildschirmsperre und automatischem Abmelden.
Konfigurieren der Projektsicherheit	Zugriff festlegen.
Konfigurieren der Instrument-Workstations	Hinzufügen des Zugriffs auf eine Workstation oder für die Zugriff auf eine Workstation entfernen.

Speicherplatz der sicherheitsrelevanten Informationen

Wenn die Analyst MD-Software auf einem einzelnen Computer oder in einer Netzwerkkonfiguration ausgeführt wird, dann werden alle Sicherheitsinformationen in der Datei `SecurityDB.odb` in folgendem Ordner auf dem Computer gespeichert:

- `C:\Program Files (x86)\Analyst\Bin`

Über Sicherheitsmodi und Konten

Dieser Abschnitt beschreibt die Optionen auf der Registerkarte „Security“ im Dialogfeld „Security Configuration“.

Single User Mode: Der aktuell unter Windows als Analyst MD Software-Administrator angemeldete Benutzer hat vollen Zugriff auf alle Funktionen der Analyst MD Software. Jeder, der sich erfolgreich unter Windows auf dem Computer anmelden kann, verfügt über Analyst MD Software-Administratorrechte.

Integrated Mode: Der aktuell unter Windows angemeldete Benutzer hat Zugriff auf die Analyst MD Software, vorausgesetzt, der Windows-Benutzer ist auch ein gültiger Benutzer der Analyst MD Software.

Mixed Mode: Der bei der Analyst MD Software aktuell angemeldete Benutzer kann entweder derselbe Benutzer oder ein anderer Benutzer als der aktuell bei Windows angemeldete Benutzer sein. Dem bei der Analyst MD Software angemeldeten Benutzer können bestimmte Rollen in der gleichen Art und Weise wie im „Integrated Mode“ zugewiesen werden. Dies ermöglicht es, dass sich bei Windows eine ganze Gruppe mit einem bekannten Passwort anmelden kann, während die Analyst MD Software verlangt, dass sich ein Benutzer bei der Analyst MD Software mit einem eindeutigen Benutzernamen, Kennwort und gegebenenfalls Domäne anmeldet.

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

Acquisition Account: Ein Netzwerkkonto für das Lesen und Schreiben von Daten in den Projektordnern bei der normalen Erfassung, nicht aber für Tuning. Der Netzwerkadministrator muss die entsprechenden Zugriffsrechte für Netzwerkkonten einrichten. Das „Acquisition Account“ verwendet die Rechte entweder vom „Client Account“ oder vom „Special Acquisition Administrator Account“.

Client Account: Verwenden Sie dasselbe Konto, das auch für die Anmeldung bei der Analyst MD Software zur Datenerfassung verwendet wurde. Im „Integrated Mode“ wird der Benutzer, der sich bei Windows angemeldet hat, auch bei der Analyst MD Software angemeldet. Im „Mixed Mode“ kann der Windows-Benutzer ein anderer sein als der bei der Analyst MD Software angemeldete Benutzer.

Special Acquisition Administrator Account: Bei der Verwendung der Analyst MD Software wird eine Netzwerkerfassung nicht empfohlen. Diese Funktion ist für die Verwendung in einem regulierten Umfeld bestimmt. Der Betreiber muss für dieses Konto einen Benutzernamen, die Domäne und das Kennwort eingeben. Nachdem der Netzwerk-Administrator dieses Konto eingerichtet hat, kann es unabhängig von der Identität des aktuellen Benutzers der Analyst MD Software zur Datenerfassung verwendet werden. Obwohl der aktuelle Benutzer keine Rechte zur Änderung von Daten im Datenordner haben könnte, kann die Datenerfassung trotzdem stattfinden. Die Kontoinformationen sind verschlüsselt und werden in der Registry gespeichert. Siehe Abschnitt: Besonderes Erfassungskonto.

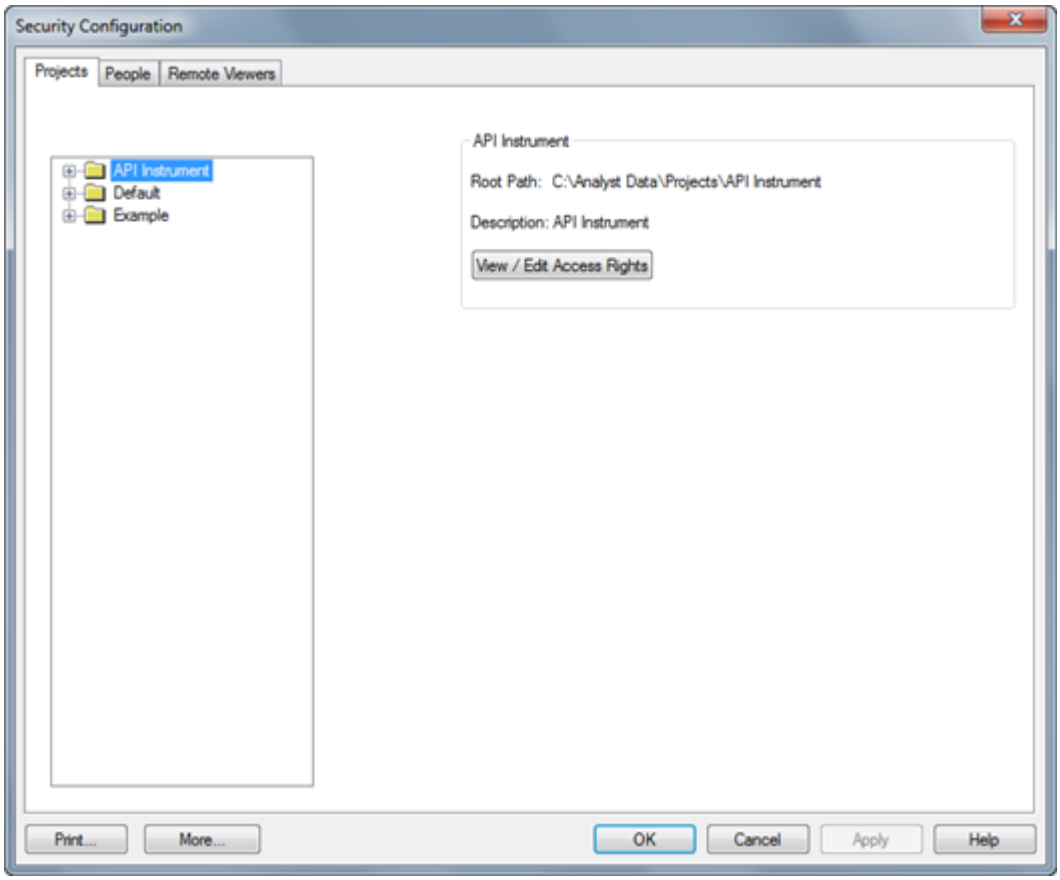
Screen Lock and Auto Logout: Aus Sicherheitsgründen kann der Computerbildschirm nach Ablauf einer bestimmten Zeit der Inaktivität gesperrt werden. Es kann zudem eine

automatische Logout-Zeit festgelegt werden, sodass sich der Analyst MD Software-Client nach einer bestimmten Zeit der Inaktivität abmeldet. „Screen Lock“ und „Auto Logout“ sind nur im „Mixed Mode“ verfügbar.

Auswählen des Sicherheitsmodus

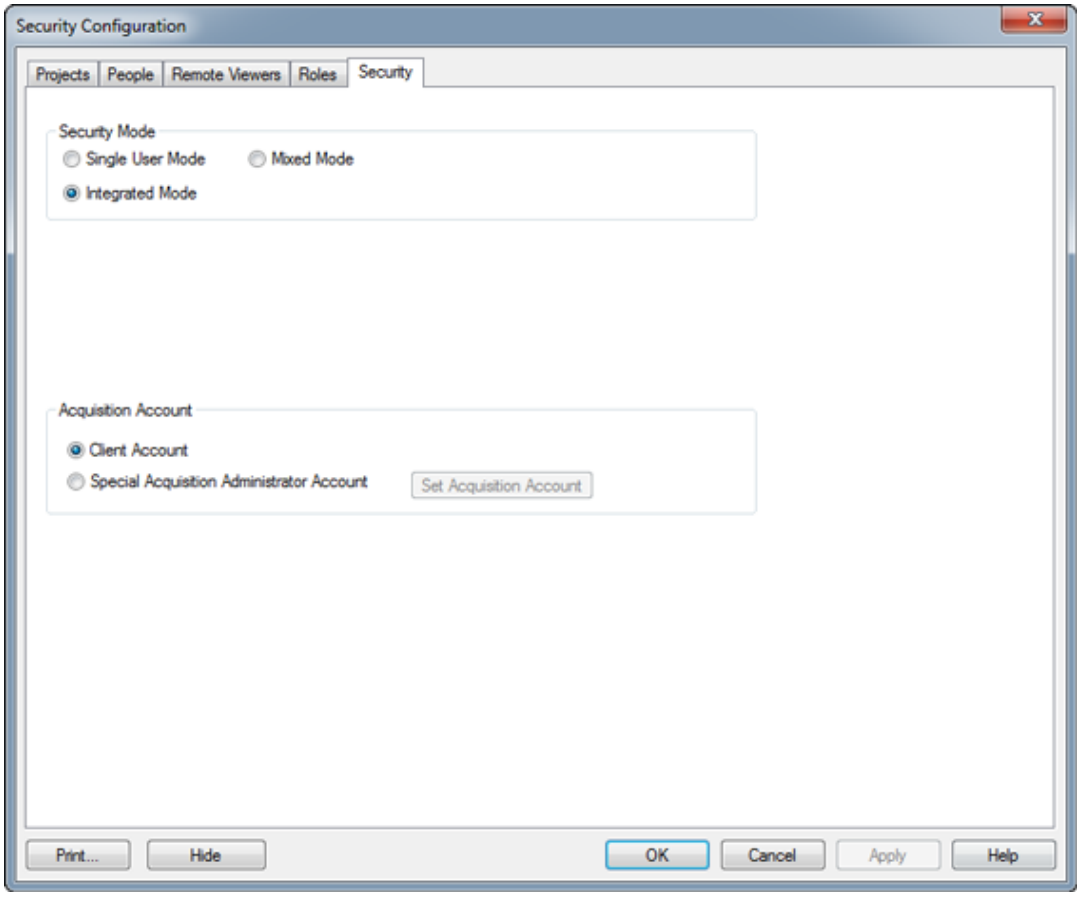
1. Doppelklicken Sie in der Navigationsleiste unter **Configure** auf **Security Configuration**.

   Abbildung 5-1: Dialogfeld „Security Configuration“: Registerkarte „Projects“



2. Klicken Sie auf **More** und öffnen Sie dann die Registerkarte „Security“.

Abbildung 5-2: Dialogfeld „Security Configuration“: Registerkarte „Security“



3. Klicken Sie in der Gruppe „Security Mode“ auf einen Modus und klicken Sie dann auf **OK**.
4. Starten Sie die Analyst MD Software neu.

Ein Erfassungskonto auswählen

1. Doppelklicken Sie in der Navigationsleiste unter **Configure** auf **Security Configuration**.
2. Klicken Sie auf **More** und öffnen Sie dann die Registerkarte „Security“.
3. In der Gruppe „Acquisition Account“ wählen Sie ein Erfassungskonto aus.
4. Wenn **Special Acquisition Administrator Account** ausgewählt ist, dann gehen Sie wie folgt vor:

   a. Klicken Sie auf **Set Acquisition Account**.

   b. Geben Sie den **User name**, das **Password** und gegebenenfalls die **Domain** ein und klicken dann auf **OK**.

   Wenn „Active Directory“ in der systemeigenen Umgebung verwendet wird, ist das Feld „Domain“ nicht sichtbar und der Benutzername kann im UPN-Format eingegeben werden.

5. Klicken Sie auf **OK**.

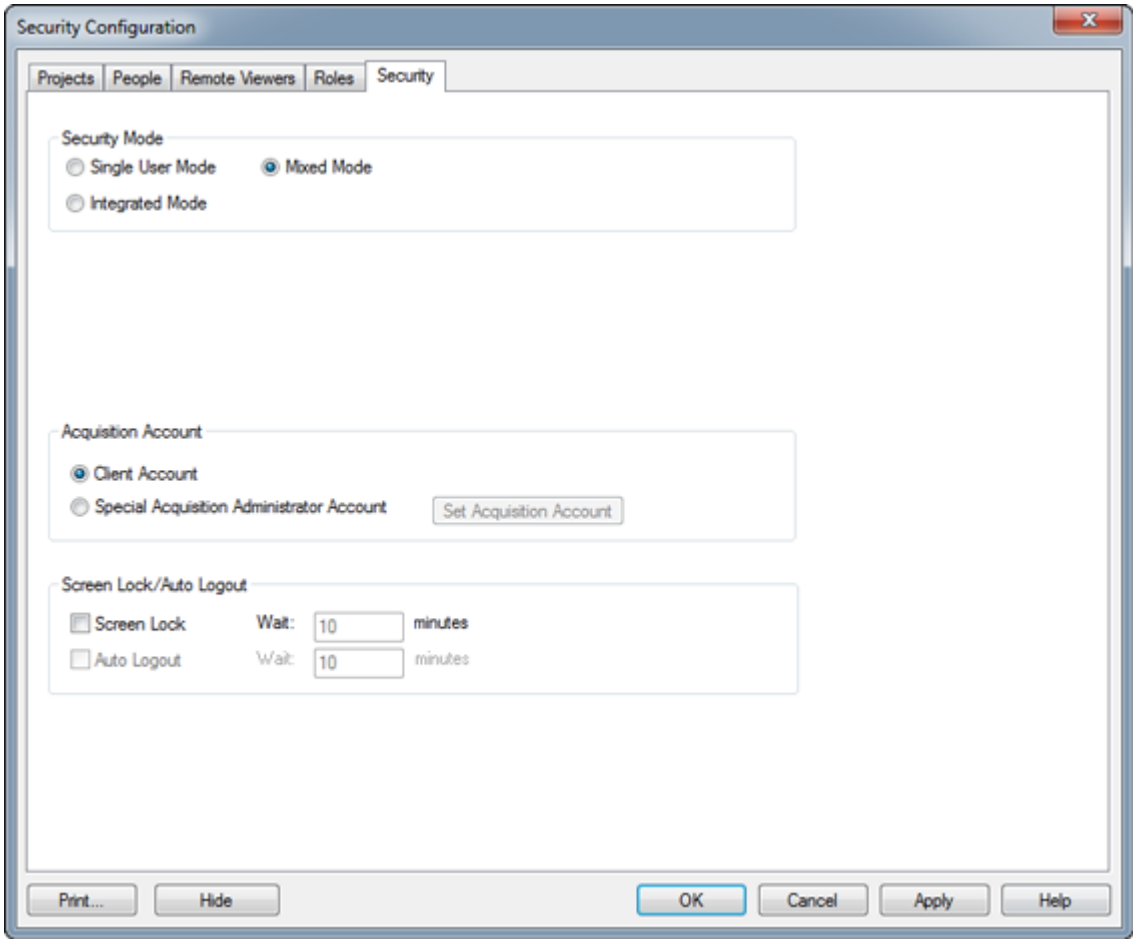
Einrichten von Bildschirmsperre und automatischem Abmelden

Wenn der Bildschirm gesperrt wird, zeigt das Dialogfeld „Unlock Analyst“ an, dass das System gesperrt wurde, sowie den derzeit angemeldeten Benutzernamen mit Domäne. Wenn die Option „Auto Logout“ ebenfalls gesetzt ist, dann wird auch die noch verbleibende Zeit angezeigt, bevor die Analyst MD Software geschlossen wird. Nur der aktuell angemeldete Benutzer oder Benutzer mit Administrator- oder Supervisor-Rollen können die Analyst MD Software entsperren oder schließen.

Hinweis: Screen Lock und **Auto Logout** sind nur im Mixed Mode verfügbar.

1. Doppelklicken Sie in der Navigationsleiste unter **Configure** auf **Security Configuration**.
2. Klicken Sie auf **More** und öffnen Sie dann die Registerkarte „Security“.
3. Klicken Sie auf **Mixed Mode**.

Abbildung 5-3: Dialogfeld „Security Configuration“: Registerkarte „Security“



4. Aktivieren Sie das Kontrollkästchen **Screen Lock**.

5. Geben Sie im Feld **Wait** die Anzahl der Minuten ein, die verstreichen müssen, bevor der Bildschirm gesperrt wird.

   Hinweis: Wenn „Auto Logout“ aktiviert ist und der Bildschirm nicht entsperrt wird, dann wird der Analyst MD Software-Client geschlossen. Wenn eine Erfassung durchgeführt wird, wird sie fortgeführt. Ist jedoch eine „Results Table“, der „Method Editor“ oder irgendeine andere Anwendung noch offen und nicht gespeichert, gehen alle Änderungen und nicht gespeicherten Daten verloren.

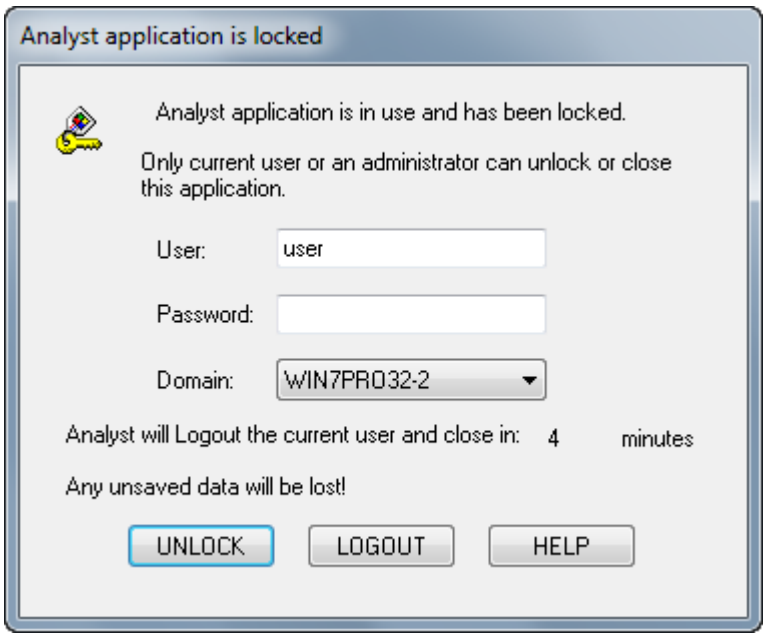
6. Falls erforderlich wählen Sie **Auto Logout** und im Feld **Wait** geben Sie die Anzahl der Minuten ein die verstreichen muss, bevor der Analyst MD Software-Client geschlossen wird.

   Der Benutzer hat eine 10-Sekunden-Frist, um die Maus zu bewegen oder eine Taste zu drücken, um das Dialogfeld „Unlock Analyst“ zu schließen. Nur der aktuell angemeldete Benutzer oder Benutzer mit Administrator- oder Supervisor-Rollen können die Analyst MD Software entsperren oder schließen. Das Dialogfeld „Unlock Analyst“ zeigt auch die noch verbleibende Zeit an, bevor der Benutzer ausgeloggt wird.

Entsperren oder Abmelden von der Analyst MD Software

Wenn „Screen Lock“ aktiviert ist, dann öffnet sich das Dialogfeld „Unlock Analyst“ nach Ablauf der „Screen Lock time“.

Abbildung 5-4: Dialog „Unlock Analyst“



Führen Sie einen der folgenden Schritte aus:

- Um den Bildschirm zu entsperren, geben Sie den Benutzernamen und gegebenenfalls das Kennwort ein und klicken dann auf **UNLOCK**.
- Um sich abzumelden, geben Sie den Benutzernamen und gegebenenfalls das Kennwort ein und klicken Sie dann auf **LOGOUT**.

Zugriff auf die Analyst MD-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 konfiguriert, **abservice**. Dieses Konto wird vom SCIEX-Dienst 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 Analyst MD-Softwarebereitstellung die Gruppenrichtlinien mit dem Active-Directory-Administrator.

Über Benutzer und Rollen

Die Analyst MD Software beschränkt den Zugriff auf Personen mit der Berechtigung, sich am Computer und bei der Analyst MD Software mit ihrem Windows-Benutzernamen und -Kennwort für Software und Computer anzumelden; dies gilt nicht für den Mixed Modus. Die Analyst MD Software erlaubt nicht mehrere Sitzungen gleichzeitig.

Hinweis: Die Registerkarten „People“ und „Role“ sind im „Single User“-Modus nicht verfügbar.

Ein Analyst MD Software-Administrator kann Windows-Benutzer und -Gruppen zur Analyst MD Software-Sicherheitsdatenbank hinzufügen. Personen oder Gruppen müssen einer der sechs vordefinierten Rollen zugewiesen werden oder neue Rollen können, falls notwendig, erstellt werden. Die vordefinierten Rollen können nicht gelöscht aber ihre Rechte können geändert werden. Nur Benutzer mit Analyst MD Software-Rollen können auf Analyst MD Software-Komponenten zugreifen.

Tabelle 5-2: Analyst MD Software Rollen

Rolle	Typische Aufgaben	Voreinstellung Zugriff
Administrator	• Verwaltet das System. • Konfiguriert die Sicherheit.	• Alle Funktionen der Analyst MD Software
Analyst	• Überwacht den Massenspektrometer-Betrieb • Analysiert Daten zur Verwendung durch den Endbenutzer.	• Erfassungsmethode • Analyst-Anwendung • Audit Trail Manager • Compound Database (Datenbank für chemische Verbindungen) • Explore (untersuchen) • Hardwarekonfiguration • Quantifizierung • Report Template Editor • Probenwarteschlange • Tune (optimieren, abstimmen) • Status anzeigen
Operator	Überwacht den täglichen Gebrauch des Systems einschließlich Wartung, Proben-Organisation, Datenerfassung und Verarbeitung	• Erfassungsmethode • Analyst-Anwendung • Audit Trail Manager • Charge • Compound Database (Datenbank für chemische Verbindungen) • Explore (untersuchen) • ExpressView („Legacy“-Einstellung[1]) • Hardwarekonfiguration • Report Template Editor • Probenwarteschlange • Tune (optimieren, abstimmen) • Status anzeigen

[1] Diese Funktion wird nicht unterstützt von der Analyst MD Software.

Tabelle 5-2: Analyst MD Software Rollen (Fortsetzung)

Rolle	Typische Aufgaben	Voreinstellung Zugriff
End User	• Liefert Proben • Erhält die Ergebnisse der Verarbeitung • Integriert die Ergebnisse mit den Ein- und Ausgaben bei anderen Anwendungen	• Erfassungsmethode • Analyst-Anwendung • Audit Trail Manager • Compound Database (Datenbank für chemische Verbindungen) • Explore (untersuchen) • ExpressView („Legacy“-Einstellung[1]) • Report Template Editor • Status anzeigen
QA Reviewer	• Prüft Daten. • Prüft Audit-Trails. • Bewertet Quantifizierungsergebnisse.	• Analyst-Anwendung • Audit Trail Manager • Quantifizierung • Report Template Editor • Status anzeigen
Supervisor	Entsperrt Software oder meldet Benutzer ab	• Entsperr- und Abmelde-Anwendung

Analyst MD Software-Zugriff

Abbildung 5-5: Dialogfeld „Security Configuration“

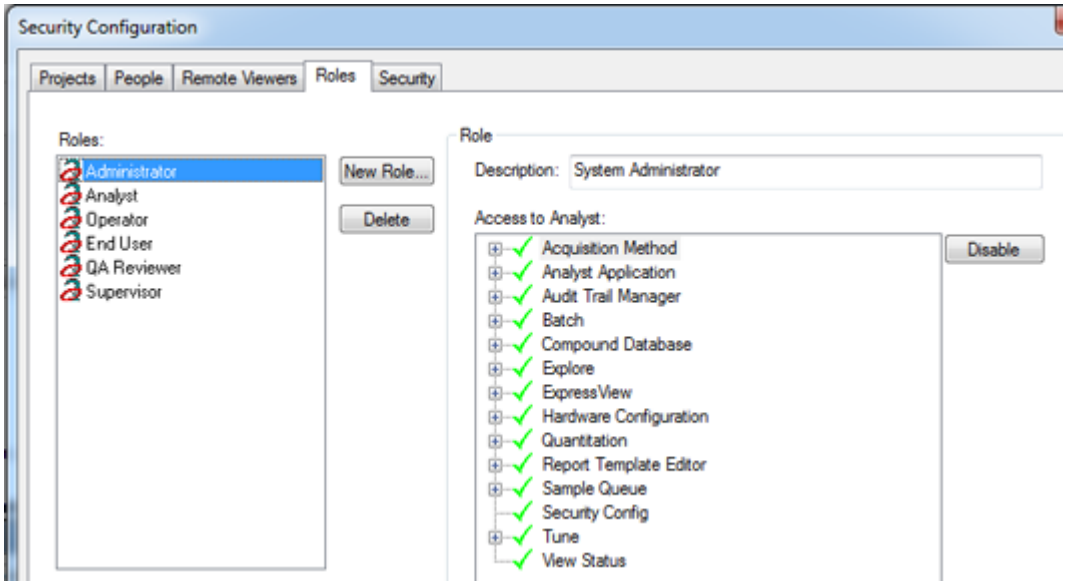


Tabelle 5-3: Analyst MD Software-Zugriff auf Erfassungsmethoden

Voreinstellung Zugriff	Beschreibung
Create/save acquisition methods	Ermöglicht Benutzern das Erstellen und Speichern von Erfassungsmethoden.
Open acquisition methods as read-only (acquire mode)	Ermöglicht Benutzern Erfassungsmethoden im schreibgeschützten Modus zu öffnen, wenn die Optionen **Create/save acquisition methods** und **Overwrite acquisition methods** deaktiviert sind.
Overwrite acquisition methods	Ermöglicht Benutzern Erfassungsmethoden zu überschreiben.

Tabelle 5-4: Analyst MD Software-Zugriff auf Analyst-Anwendung

Voreinstellung Zugriff	Beschreibung
Use Workspace functions[2]	Ermöglicht es Benutzern, Workspace-Funktionen zu verwenden.
Create Project	Ermöglicht Benutzern das Erstellen von Projekten.
Copy Project	Ermöglicht Benutzern das Kopieren von Projekten.

Tabelle 5-4: Analyst MD Software-Zugriff auf Analyst-Anwendung (Fortsetzung)

Voreinstellung Zugriff	Beschreibung
Create Root Directory	Ermöglicht es Benutzern, ein Stammverzeichnis zu erstellen.
Set Root Directory	Ermöglicht es Benutzern, das Stammverzeichnis festzulegen.
Change Project	Ermöglicht es Benutzern, das Projekt zu ändern.
Load/Save Processed Data Files	Ermöglicht Benutzern das Laden und Speichern von verarbeiteten Dateien.
Lock/Logout Application	Ermöglicht das automatische Sperren der Anwendung oder das automatische Abmelden des Benutzers, nachdem eine bestimmte Zeit der Inaktivität abgelaufen ist. Diese Funktion steht nur im „Mixed“-Modus zur Verfügung, und wenn die Option **Screen Lock** oder **Auto Logout** ausgewählt wurde.

Tabelle 5-5: Analyst MD Software-Zugriff auf Audit Trail Manager

Voreinstellung Zugriff	Beschreibung
View Audit Trail Data	Ermöglicht Benutzern, die „Audit-Trail“-Daten anzuzeigen. Deaktivieren Sie den Zugriff auf diese Berechtigung für alle Benutzer, mit Ausnahme der Administratoren.
Change Audit Trail Settings	Ermöglicht es Benutzern, die Audit-Trail-Einstellungen zu ändern.
Maintenance Log	Ermöglicht Benutzern das Anzeigen des Wartungsprotokolls.
Create or Modify Audit Maps	Ermöglicht Benutzern das Erstellen oder Ändern von Audit Maps.

Tabelle 5-6: Analyst MD Software-Zugriff auf Charge

Voreinstellung Zugriff	Beschreibung
Open existing batches	Ermöglicht Benutzern das Öffnen einer bestehenden Charge.
Create new batches	Ermöglicht es Benutzern, eine Charge zu erstellen.

Tabelle 5-6: Analyst MD Software-Zugriff auf Charge (Fortsetzung)

Voreinstellung Zugriff	Beschreibung
Import	Ermöglicht es Benutzern, Daten aus einer vorhandenen Charge (mdb oder andere unterstützte Dateiformate) zu importieren.
Save batches	Ermöglicht es Benutzern, eine Charge zu speichern.
Use template batches	Ermöglicht es Benutzern, Chargen-Vorlagen zu speichern oder zu öffnen.
Edit batches	Ermöglicht es Benutzern, eine Charge zu bearbeiten.
Submit batches	Ermöglicht Benutzern das Übergeben einer Charge.
Add or remove custom columns	Ermöglicht Benutzern das Hinzufügen oder Entfernen von benutzerdefinierten Spalten aus dem Batch Editor.
Use template acquisition methods	Ermöglicht es Benutzern, eine Erfassungsmethode als Vorlage zu verwenden. Diese Option ist im Batch Editor verfügbar. Sobald eine Methode ausgewählt ist, wird die Option **Use as template**aktiviert.
Overwrite batches	Ermöglicht es Benutzern, vorhandene Chargen zu überschreiben.
Overwrite template batches	Ermöglicht es Benutzern, vorhandene Chargen-Vorlagen zu überschreiben.

Tabelle 5-7: Analyst MD Software-Zugriff auf Datenbank für chemische Verbindungen

Voreinstellung Zugriff	Beschreibung
Setup compound database location	Stellt die Optionen für den Speicherplatz und den Namen der Verbindung auf „ReadOnly“ (schreibgeschützt) und deaktiviert die Schaltfläche „Browse“. (Im Explore-Modus, klicken Sie auf **Tools** > **Settings** > **Optimization Options**.) Aktiviert die Schaltfläche **Use Defaults Now** im Dialogfeld „Optimization Options“ nur dann, wenn der Benutzer sowohl Zugriff auf die Datenbank für chemische Verbindungen als auch auf die Benutzeroptionen für die Datenbank für chemische Verbindungen hat.

Tabelle 5-7: Analyst MD Software-Zugriff auf Datenbank für chemische Verbindungen (Fortsetzung)

Voreinstellung Zugriff	Beschreibung
Setup user options	Ermöglicht Benutzern die Optionen für Benutzer-ID und Kennwort im Dialogfeld „Optimization Options“ einzustellen. (Im Explore-Modus, klicken Sie auf **Tools** > **Settings** > **Optimization Options**.) Aktiviert die Schaltfläche **Use Defaults Now** im Dialogfeld „Optimization Options“ nur dann, wenn der Benutzer sowohl Zugriff auf die Datenbank für chemische Verbindungen als auch auf die Benutzeroptionen für die Datenbank für chemische Verbindungen hat. (Durch einen Klick mit der rechten Maustaste in die Datenbank für chemische Verbindungen - Compound Database - erhalten Sie Zugriff auf diese Funktionen.)
Add to compound database	Ermöglicht es Benutzern, Verbindungen zur Datenbank für chemische Verbindungen hinzuzufügen. (Durch einen Klick mit der rechten Maustaste in die Datenbank für chemische Verbindungen - Compound Database - erhalten Sie Zugriff auf diese Funktion.)
Modify database (overrides add/ delete if disabled)	Ermöglicht Benutzern das Hinzufügen, Löschen oder Ändern der Datenbank für chemische Verbindungen (Einstellungen für Verbindungen oder Optimieren).
Delete compound from database	Ermöglicht es Benutzern, Verbindungen aus der Datenbank für chemische Verbindungen zu löschen. (Durch einen Klick mit der rechten Maustaste in die Datenbank für chemische Verbindungen - Compound Database - erhalten Sie Zugriff auf diese Funktion.)
Delete optimization settings from database	Ermöglicht Benutzern, Einstellungen für die Optimierung aus der Datenbank für chemische Verbindungen zu löschen. (Durch einen Klick mit der rechten Maustaste in die Datenbank für chemische Verbindungen - Compound Database - erhalten Sie Zugriff auf diese Funktion.)

Tabelle 5-8: Analyst MD Software-Zugriff auf Explore

Voreinstellung Zugriff	Beschreibung
Save data to text file	Ermöglicht es Benutzern, Daten in Textdateien zu speichern. (Mit der rechten Maustaste in ein Spektrum oder Chromatogramm klicken und dann auf **Save to Text File** klicken.)
Setup library location	Ermöglicht es Benutzern, den Speicherort der „Library Database“ einzurichten oder auszuwählen.
Setup library user options	Ermöglicht es Benutzern, Sicherheitsinformationen wie Benutzername und Passwort für die Bibliothek einzurichten.

Tabelle 5-8: Analyst MD Software-Zugriff auf Explore (Fortsetzung)

Voreinstellung Zugriff	Beschreibung
Add library record	Ermöglicht es Benutzern, einen Bibliothek-Datensatz hinzuzufügen. (Klicken Sie mit der rechten Maustaste in ein Spektrum oder klicken Sie im Explore-Modus auf **Explore** > **Library Search** > **Add**.)
Add spectrum to library record	Wenn diese Option deaktiviert ist, können Benutzer im Dialogfeld „Library Search“ nicht auf die Schaltfläche „Append MS“ klicken. (Im Explore-Modus, klicken Sie auf **Explore** > **Library Search** > **List**.)
Modify library record (overrides add/ delete if disabled)	Ermöglicht es Benutzern, Bibliotheksdatensätze zu ändern.
Delete MS spectrum	Ermöglicht es Benutzern, ein ausgewähltes MS-Spektrum zu löschen.
Delete UV spectrum	Ermöglicht es Benutzern, ein UV-Spektrum zu löschen.
Delete structure	Ermöglicht es Benutzern, eine Struktur zu löschen.
View library	Ermöglicht es Benutzern, die Funktion „List“ und „List with Constraints“ zu nutzen. (Im Explore-Modus, klicken Sie auf **Explore** > **Library Search**.)
Search library	Ermöglicht Benutzern die Verwendung der Funktionen „Search Library“ und „Set Search Constraints“. (Klicken Sie mit der rechten Maustaste in ein Spektrum oder im Explore-Modus auf **Explore** > **Library Search**.)
Select processing algorithm to retrieve peak list	„Legacy“-Einstellung[2]

Tabelle 5-9: Analyst MD Software-Zugriff auf ExpressView*

Voreinstellung Zugriff	Beschreibung
Start Express View dialog	„Legacy“-Einstellung[2]
Modify options	„Legacy“-Einstellung[2]

[2] Diese Funktion wird nicht unterstützt von der Analyst MD Software.

Tabelle 5-10: Analyst MD Software-Zugriff auf Hardwarekonfiguration

Voreinstellung Zugriff	Beschreibung
Create	Ermöglicht es Benutzern, ein Hardwareprofil zu erstellen.
Delete	Ermöglicht es Benutzern, ein Hardwareprofil zu löschen.
Edit	Ermöglicht es Benutzern, ein Hardwareprofil zu bearbeiten.
Activate/ Deactivate	Ermöglicht es Benutzern, ein Hardwareprofil zu aktivieren oder zu deaktivieren.

Tabelle 5-11: Analyst MD Software-Zugriff auf Quantifizierung

Voreinstellung Zugriff	Beschreibung
Create quantitation method	Ermöglicht es Benutzern, neue Quantifizierungsmethoden zu erstellen.
Change default method options	Ermöglicht es Benutzern, die Standard-Methode zu ändern.
Use full method editor	Ermöglicht es Benutzern, den Quantitation Method Editor zu verwenden.
Create “automa tic” methods	Ermöglicht es Benutzern, eine Quantifizierungsmethode innerhalb des Quantifizierungsassistenten zu erstellen.
Modify existing methods	Ermöglicht es Benutzern, bestehende Quantifizierungsmethoden zu ändern (zu überschreiben).
Change peak names (in wizard)	Ermöglicht es Benutzern, Peak-Namen im Quantifizierungsassistenten zu ändern.
Change default number of smooths (in wizard)	Ermöglicht es Benutzern, die Standardanzahl der Glättungen im „Quantitation Wizard“ zu spezifizieren.
Change “advan ced” parameters (in wizard)	Ermöglicht Benutzern, die erweiterten Parameter im Quantifizierungsassistenten zu ändern. Wenn Benutzer nicht über diese Option verfügen, wird die Schaltfläche „Advanced“ ausgeblendet.
Change concentration units (in wizard)	Ermöglicht es Benutzern, die Konzentrationseinheiten in den erweiterten Parametern im Quantifizierungsassistenten zu ändern.

Tabelle 5-11: Analyst MD Software-Zugriff auf Quantifizierung (Fortsetzung)

Voreinstellung Zugriff	Beschreibung
Create new results tables	Ermöglicht es Benutzern, eine neue „Results Table“ mit dem Quantifizierungsassistenten oder durch Auswahl von **New** im Menü **File** zu erstellen. Die Schaltfläche „ Save As“ wird durch diese Option nicht deaktiviert.
Open existing results tables	Ermöglicht es Benutzern, die bestehenden „Results Tables“ zu öffnen.
When saving, replace existing results tables	Ermöglicht es Benutzern, die bestehenden „Results Tables“ zu überschreiben.
Edit results tables’ method	Ermöglicht es Benutzern, die Quantifizierungsmethodendatei zu ändern. Klicken Sie im Quantifizierungs-Modus auf **Tools** > **Results Table** > **Modify Method**. Dies ändert die eigentliche Datei und nicht die eingebettete Methode in einer „Results Table“.
Create new “standard” queries (from wizard)	Ermöglicht es Benutzern, eine neue Standard-Abfrage mit dem Quantifizierungsassistenten zu erstellen.
Exclude standards from calibration	Ermöglicht es Benutzern, Standards im Teilfenster „Calibration Curve“ in einer „Results Table“ und im Teilfenster „Statistics“ aus Kalibrierungen auszuschließen.
Add and Remove samples from results table	Ermöglicht Benutzern das Hinzufügen oder Entfernen von Proben. (Klicken Sie im Modus **Quantitate** auf **Tools** > **Results Table** > **Add/ Remove samples**.) Deaktivieren Sie den Zugriff auf diese Berechtigung für alle Benutzer, mit Ausnahme der Administratoren.
Display metric plots	Ermöglicht es Benutzern, metrische Kurven aus einer „Results Table“ anzeigen zu lassen. (In einer „Results Table“ klicken Sie mit der rechten Maustaste und klicken dann auf **Metric Plot**.)
Create or modify formula columns	Ermöglicht es Benutzern, das Erstellen oder Ändern von Formel-Spalten in einer „Results Table“.
Modify sample name	Ermöglicht es Benutzern, Probennamen zu ändern.
Export results table as text file	Ermöglicht es Benutzern, eine „Results Table“ als Textdatei zu exportieren. (Klicken Sie im **Quantitate**-Modus bei geöffneter „Results Table“ auf **Tools** > **Results Table** > **Export as Text**.)

Tabelle 5-11: Analyst MD Software-Zugriff auf Quantifizierung (Fortsetzung)

Voreinstellung Zugriff	Beschreibung
Export settings from results table	Ermöglicht es Benutzern, Tabelleneinstellungen in neue „Results Table“-Einstellungen zu exportieren. (Klicken Sie mit der rechten Maustaste in einer „Results Table“ und klicken Sie dann auf **Table Settings** > **Export To New Table Settings**.)
Modify custom column title	Ermöglicht es Benutzern, die Spaltenüberschrift einer benutzerdefinierten Spalte zu ändern. Eine Formel-Spalte ist keine benutzerdefinierte Spalte.
Modify results table settings	Ermöglicht es Benutzern, die Tabelleneinstellungen aus einer „Results Table“ zu ändern (klicken Sie mit der rechten Maustaste und klicken Sie auf **Table Settings** > **Edit**) oder auf globale Tabelleneinstellungen (klicken Sie im **Quantitate**-Modus auf **Tools** > **Settings** > **New Quantitation Results Table Settings**.) Diese Sicherheit ist nicht erforderlich, wenn man zwischen bestehenden Tabellen wechselt.
Modify global (default) settings	Ermöglicht es Benutzern, die globalen Tabelleneinstellungen zu ändern. (Klicken Sie im Modus **Quantitate** auf **Tools** > **Settings** > **New Quantitation Results Table Settings.)**
Modify audit trail settings	Ermöglicht es Benutzern, die „Audit-Trail“-Einstellungen zu ändern.
Disable, enable and clear audit trail	„Legacy“-Einstellung[2]
Change results table column visibility	Ermöglicht es Benutzern, die Spalten auszuwählen, die in eine „Results Table“ übernommen werden sollen. (Um auf das Dialogfeld „Table Settings“ zuzugreifen, klicken Sie mit der rechten Maustaste in die „Results Table“ und klicken Sie dann auf **Table Settings** > **Edit**.)
Change results table column precision	Ermöglicht es Benutzern, die Spalten „Significant Figures“, „Scientific Notation“ oder „Precision“ in einer „Results Table“ zu ändern. (Um auf das Dialogfeld „Table Settings“ zuzugreifen, klicken Sie mit der rechten Maustaste in die „Results Table“ und klicken Sie dann auf **Table Settings** > **Edit.** Klicken Sie auf **Columns** und anschließend auf **Edit**.)
Run temporary queries	Ermöglicht es Benutzern, Abfragen auszuführen.
Modify or save queries	Ermöglicht es Benutzern, bestehende Abfragen zu ändern oder neue Abfragen zu speichern. (Um „Queries“ zu ändern, drücken Sie die Strg-Taste + rechte Maustaste in der Ergebnistabelle, klicken auf „Query“ und wählen dann eine vorhandene Abfrage.) Ermöglicht es Benutzern, Abfragen in einer Ergebnistabelle zu ändern. (Klicken Sie in einer „Results Table“ mit der rechten Maustaste und klicken Sie dann auf **Table Settings** > **Edit** > **Queries.** Wählen Sie einen vorhandenen „Query“ aus und klicken Sie dann auf **Edit**.)

Tabelle 5-11: Analyst MD Software-Zugriff auf Quantifizierung (Fortsetzung)

Voreinstellung Zugriff	Beschreibung
Run temporary sorts	Ermöglicht es Benutzern, „Queries“ zu sortieren.
Modify or save sorts	Ermöglicht es Benutzern, Sortierungen zu ändern oder zu speichern.
Use metric plot settings dialog	Ermöglicht es Benutzern, das Dialogfeld „Metric Plot“ zu verwenden.
Modify or create metric plot settings	Ermöglicht es Benutzern, neue metrische Kurven aus der „Results Table“ zu erstellen. (In der „Results Table“ klicken Sie mit der rechten Maustaste und klicken dann auf **Metric Plot** > **New**.) Ermöglicht Benutzern, metrische Kurven aus einer „Results Table“ zu ändern. (Klicken Sie in einer „Results Table“ mit der rechten Maustaste und klicken dann auf **Table Settings** > **Edit** > **Metric Plot**. Wählen Sie einen bestehenden „Metric Plot“ und klicken dann auf **Edit**.) Diese Sicherheitseinstellung verhindert nicht, dass Benutzer bestehende „Metric Plots“ ändern, indem sie einen „Metric Plot“ erzeugen, mit der rechten Maustaste in den „Plot“ klicken und dann „Edit Settings“ wählen.
Create Analyte Groups	Ermöglicht es Benutzern, Analyt-Gruppen aus einer „Results Table“ zu erstellen. (In einer „Results Table“ klicken Sie mit der rechten Maustaste und klicken dann auf **Analyte Group** > **New**.)
Modify Analyte Groups	Ermöglicht es Benutzern, Analyt-Gruppen zu ändern. (Klicken Sie in einer „Results Table“ mit der rechten Maustaste und klicken dann auf **Table Settings** > **Edit** > **Analyte Groups**. Klicken Sie auf eine bestehende Gruppe und klicken Sie dann auf **Edit**.)
Change default peak review options	Ermöglicht es Benutzern, die Standard-Peak-Einstellungen zu ändern. (Klicken Sie im Modus **Quantitate** auf **Tools** > **Settings** > **Quantitation Peak Review Settings**.)
Change “simple ” parameters in peak review	Ermöglicht es Benutzern, die einfachen Parameter im Peak Review zu ändern. Wenn ein „Peak Review“-Teilfenster geöffnet ist, sind die einfachen Parameter diejenigen Parameter, die dann sichtbar werden, wenn die Schaltfläche „Show or Hide Parameters“ einmal gedrückt wird.
Change “advan ced” parameters in peak review	Ermöglicht es Benutzern, die erweiterten Parameter im Peak Review zu ändern. Wenn ein „Peak Review“-Teilfenster geöffnet ist, sind die erweiterten Parameter diejenigen Parameter, die dann sichtbar werden, wenn die Schaltfläche „Show or Hide Parameters“ zweimal gedrückt wird.
Manually integrate	Ermöglicht es Benutzern, im „Manual Integration Mode“ Peaks im „Peak Review“-Teilfenster manuell zu integrieren.

Tabelle 5-11: Analyst MD Software-Zugriff auf Quantifizierung (Fortsetzung)

Voreinstellung Zugriff	Beschreibung
“Update” method in peak review	Ermöglicht es Benutzern, eine Methode zu aktualisieren und wieder zurückzusetzen, nachdem eine Quantifizierungsmethode für einen bestimmten Peak im „Peak Review“-Teilfenster geändert worden ist.
Add or modify annotation	Ermöglicht es Benutzern, Probenanmerkungen im „Peak Review“-Teilfenster oder -Fenster mit der „Sample Annotation“-Option aus dem Kontextmenü oder durch Hinzufügen einer „Sample Annotation“-Spalte in der „Results Table“ hinzuzufügen oder zu ändern.
Change regression parameters	Ermöglicht es Benutzern, die Regressionseinstellungen in einem „Calibration Curve“-Fenster zu ändern.
Modify Sample ID	Ermöglicht Benutzern das Hinzufügen oder Ändern der Proben-ID in einer „Results Table“.
Modify Sample Type	Ermöglicht es Benutzern, den Sample-Typ in einer „Results Table“ zu ändern.
Modify Sample Comment	Ermöglicht Benutzern das Hinzufügen oder Ändern der Proben-Bemerkung in einer „Results Table“.
Modify Weight To Volume ratio	Ermöglicht es Benutzern, das Gewicht-zu-Volumen-Verhältnis in einer „Results Table“ zu ändern.
Modify Dilution Factor	Ermöglicht es Benutzern, den Verdünnungsfaktor in einer „Results Table“ zu ändern.
Modify Analyte Concentration	Ermöglicht es Benutzern, die Analytkonzentrationen in einer „Results Table“ zu ändern.
Modify Analyte Units	„Legacy“-Einstellung[2]
Modify IS Concentration	Ermöglicht es Benutzern, die IS-Konzentrationen in einer „Results Table“ zu ändern.
Modify IS Units	„Legacy“-Einstellung[2]
Modify Processing Algorithm	Ermöglicht es Benutzern, den Quantifizierungsalgorithmus zu ändern. (Klicken Sie im Modus **Quantitate** auf **Tools** > **Settings** > **Quantitation Integration Algorithm**.)
Enable or Disable percent rule in Manual Integration	Ermöglicht es Benutzern, die manuelle Integration (Prozent-Regel) zu ändern. (Klicken Sie im Modus **Quantitate** auf **Tools** > **Settings** > **Quantitation Peak Review Settings**.)

Tabelle 5-12: Analyst MD Software-Zugriff auf Report Template Editor (Berichtsvorlagen-Editor oder Vorlagen-Editor)

Voreinstellung Zugriff	Beschreibung
Create/modify report templates	Ermöglicht es Benutzern, neue Berichtsvorlagen zu erstellen und die bestehenden zu ändern.
Open report templates as read-only	Ermöglicht es Benutzern, .rpt-Dateien im schreibgeschützten Format zu öffnen. (Klicken Sie auf **File** > **Open**.)
Print	Ermöglicht es Benutzern, in jedem Modus zu drucken.
Select report templates	Ermöglicht es Benutzern, bestehende Berichtsvorlagen im Dialogfeld „Print“ auszuwählen.

Tabelle 5-13: Analyst MD Software-Zugriff auf Proben-Warteschlange

Voreinstellung Zugriff	Beschreibung
Start Sample	Ermöglicht es Benutzern, eine Probe in der Warteschlange zu starten.
Abort Sample	Ermöglicht es Benutzern, eine Probe in der Warteschlange abzubrechen.
Stop Sample	Ermöglicht es Benutzern, eine Probe in der Warteschlange zu stoppen.
Stop Queue	Ermöglicht es Benutzern, eine Warteschlange zu stoppen.
Pause Sample Now[2]	Ermöglicht Benutzern das sofortige Anhalten einer Probe.
Insert Pause Before Selected Sample(s)[2]	Ermöglicht es Benutzern, eine Pause vor der nächsten Probe einzufügen.
Continue Sample[2]	Ermöglicht es Benutzern, mit einer aktuellen Probe fortzufahren (neu zu starten).
Next Period[2]	Ermöglicht es Benutzern, den nächsten Zeitabschnitt sofort zu erfassen.
Extend Period[2]	Ermöglicht es Benutzern, den derzeit erfassten Zeitabschnitt zu verlängern.
Next Sample[2]	Ermöglicht es Benutzern, die nächste Probe sofort zu erfassen.
Advance Pump Gradient	„Legacy“-Einstellung[2]
Equilibrate	Ermöglicht es Benutzern, das System zu äquilibrieren.
Stand By	Ermöglicht es Benutzern, das Massenspektrometer in den Standby-Modus zu versetzen.

Tabelle 5-13: Analyst MD Software-Zugriff auf Proben-Warteschlange (Fortsetzung)

Voreinstellung Zugriff	Beschreibung
Ready	Ermöglicht es Benutzern, das Massenspektrometer in Betriebsbereitschaft zu versetzen.
Reacquire	Ermöglicht es Benutzern, Proben erneut zu erfassen.
Insert Pause[2]	Ermöglicht es Benutzern, eine Pause in der Warteschlange einfügen.
Delete Sample or Batch	Ermöglicht es Benutzern, eine Probe oder eine Charge in der Warteschlange zu löschen.
Move Batch	Ermöglicht es Benutzern, die Chargen-Reihenfolge in der Warteschlange zu ändern.

Tabelle 5-14: Analyst MD Software-Zugriff auf Tune (Abstimmen, Feinabstimmung)

Voreinstellung Zugriff	Beschreibung
Edit parameter settings	Ermöglicht es Benutzern, die Parameter-Einstellungen zu bearbeiten. (Klicken Sie im „Calibrate“-Modus auf **Tools** > **Settings** > **Parameter Settings**.)
Edit tuning options	Ermöglicht es Benutzern, Referenztabellen für Kalibrierstandards zu erstellen, zu löschen und zu aktualisieren, und die „Offset Drops“ von der Einheitsauflösung für niedrige und offene Auflösungen zu bearbeiten.
Edit instrument data	Ermöglicht es Benutzern, Massenspektrometer-Kalibrierungs- und Auflösungstabellen zu ändern.
Manual tune	Ermöglicht es Benutzern, die manuelle Tuning-Funktion im „Tune and Calibrate“-Modus zu verwenden.
Calibrate from current spectrum	Ermöglicht Benutzern die Kalibrierung mit dem aktuellen Spektrum.
Instrument optimization	Ermöglicht es Benutzern, die Funktion „Instrument Optimization“ im „Tune and Calibrate“-Modus zu verwenden.
Compound optimization	Ermöglicht es Benutzern, die „Compound Optimization“-Funktion auszuführen.
Tuning Instrument	Ermöglicht es Benutzern, das Massenspektrometer abzustimmen und zu kalibrieren.
Advanced Resolution Table Modification	Ermöglicht Benutzern die Auflösung mit der Schaltfläche „Advanced“ in der Registerkarte „Resolution“ zu konfigurieren.

Tabelle 5-14: Analyst MD Software-Zugriff auf Tune (Abstimmen, Feinabstimmung) (Fortsetzung)

Voreinstellung Zugriff	Beschreibung
Auto TOF Mass Calibration	„Legacy“-Einstellung[2]

Tabelle 5-15: Analyst MD Software-Zugriffsrechte

Voreinstellung Zugriff	Beschreibung
Security Config	Ermöglicht es Benutzern, sicherheitsrelevante Einstellungen zu konfigurieren.
View Status	Ermöglicht es Benutzern, den Status von Remote-Massenspektrometern anzuzeigen.

Hinweis: Falls Formelspalten erstellt oder verwendet werden, empfehlen wir, dass die Benutzer diese Formeln vor deren Verwendung validieren.

MultiQuant MD Software-Zugriff

Voreinstellung Zugriff	Beschreibung
Create session file	Ermöglicht es den Benutzern, eine „Results Table“ zu erstellen.
Create quantitation method	Ermöglicht es den Benutzern, Quantifizierungsmethoden zu erstellen.
Modify quantitation method files	Ermöglicht es den Benutzern, die Quantifizierungsmethoden im Ordner „Quantitation Methods“ im Ordner „Analyst Data“ zu ändern.
Allow Export and Create Report of unlocked Results Table	Ermöglicht es den Benutzern, Berichte aus nicht gesperrten Results Table zu erstellen oder exportieren.
Create automatic method	Ermöglicht es Benutzern, die Option „Automatic Method“ beim Erstellen von „Results Tables“ auszuwählen.

Voreinstellung Zugriff	Beschreibung
Replace existing Results Table when saved	Ermöglicht es den Benutzern, vorhandene „Results Tables“ zu aktualisieren, aber erlaubt ihnen nicht, eine neue „Results Table“ mit dem Namen einer vorhandenen „Results Table“ zu erstellen. Wenn zum Beispiel eine „Results Table“ mit dem Namen RT1 erstellt wird, können die Benutzer sie aktualisieren, aber sie können keinen neue „Results Table“ mit dem Namen RT1 erstellen. Die Benutzer können keine unbenannte „Results Table“ mit dem Namen einer vorhandenen „Results Table“ benennen.
Change default quantitation method integration algorithm	Ermöglicht es den Benutzern, den Algorithmus im Dialogfeld „Integration Default“ zu ändern. (Klicken Sie auf **Edit** > **Project Integration Defaults**.)
Change default quantitation method integration parameters	Ermöglicht es den Benutzern, die Standardparameter des Algorithmus im Dialogfeld „Integration Default“ zu ändern. (Klicken Sie auf **Edit** > **Project Integration Defaults**.)
Allow Enable Project Modified Peak Warning	Ermöglicht es den Benutzern, die Kennzeichnung zu aktivieren, die die Option „Project Modified Peak Warning“ im Menü „Edit“ aktiviert.
Add samples to Results Table	Ermöglicht Benutzern das Hinzufügen von Proben. (Klicken Sie auf **Process** > **Add Samples**.)
Remove samples from Results Table	Ermöglicht es den Benutzern, ausgewählte Proben zu entfernen. (Klicken Sie auf **Process** > **Remove Selected Samples**.)
Export, import, or remove External Calibration	Ermöglicht es den Benutzern, eine externe Kalibrierung mit einer der folgenden Optionen zu exportieren, zu importieren oder zu entfernen: • Klicken Sie auf **Process** > **Export Calibration**. • Klicken Sie auf **Process** > **Import External Calibration**. • Klicken Sie auf **Process** > **Remove External Calibration**.
Use, edit, or clear Isotopic Correction	Ermöglicht den Benutzern die Verwendung, Bearbeitung oder das Löschen einer Isotopenkorrektur mithilfe einer der folgenden Optionen: • Klicken Sie auf **Process** > **Use Default Isotope Correction**. • Klicken Sie auf **Process** > **Edit Current Isotope Correction**. • Klicken Sie auf **Process** > **Clear Previous Isotope Correction**.

Voreinstellung Zugriff	Beschreibung
Change Audit Map settings	Ermöglicht es den Benutzern, die Audit Map des Projekts und die Audit Map-Definition zu ändern. (Klicken Sie auf **Audit Trail** > **Audit Map Manager**.)
Modify Sample Name	Ermöglicht Benutzern das Ändern der Probennamen in der „Results Table“.
Modify Sample Type	Ermöglicht es den Benutzern, die Probenart (Standard, QC, Unknown) in der „Results Table“ zu ändern.
Modify Sample ID	Ermöglicht Benutzern das Ändern der Proben-ID in der „Results Table“.
Modify Actual Concentration	Ermöglicht Benutzern das Ändern der tatsächlichen Konzentration von Standard und Qualitätskontrolle in der „Results Table“.
Modify Dilution Factor	Ermöglicht Benutzern das Ändern des Verdünnungsfaktors in der „Results Table“.
Modify Comment Fields	Ermöglicht Benutzern das Ändern von Kommentarfeldern: • Component Comment • IS Comment • IS Peak Comment • Peak Comment • Sample Comments
Allow manual integration	Ermöglicht es den Benutzern, den manuellen Integrationsmodus unter „Peak Review“ zu aktivieren.
Allow set to Peak Not Found	Ermöglicht es den Benutzern, die Funktion „Set peak to not found“ unter „Peak Review“ zu verwenden. Klicken Sie dazu mit der rechten Maustaste im Fenster „Peak Review“.
Include or exclude a peak from the Results Table	Ermöglicht es den Benutzern, Peaks aus „Results Tables“, „Statistics Tables“ und „Calibration Curves“ ein- oder auszuschließen.
Modify regression settings for fit and weight	Ermöglicht es den Benutzern, die Regressionseinstellungen im Fenster „Calibration Curve“ zu ändern, wenn die Funktion „Modify Results Table Method“ und der „New Quantitation Method“ Assistent verwendet werden.

Voreinstellung Zugriff	Beschreibung
Modify Results Table integration parameters for a single chromatogram	Ermöglicht es dem Benutzer, ein einzelnes Chromatogramm zu ändern.
Modify quantitation method for the Results Table component	Ermöglicht es dem Benutzer, die Änderungen von den einzelnen Chromatogrammen auf die Komponente anzuwenden. Die Benutzer müssen über diese Berechtigung verfügen und die Berechtigung „Modify Results Table integration parameters for a single chromatogram“ muss aktiviert sein, wenn sie einzelne Änderungen auf Komponenten anwenden möchten.
Create, use, or export Metric Plots in Results Tables	Ermöglicht es den Benutzern, metrische Kurven in der „Results Table“ zu erstellen und zu verwenden (Schaltfläche „Metric Plot“ ist aktiviert) oder metrische Kurven zu exportieren. (Klicken Sie auf **File** > **Export**.)
Set Peak Review Title Format	Ermöglicht es den Benutzern, das „Peak Review Title Format“ in „Peak Review“ zu ändern. Klicken Sie dazu mit der rechten Maustaste im Fenster „Peak Review“.
Add, Rename, or Modify custom column	Ermöglicht es den Benutzern, benutzerdefinierte Spalten hinzuzufügen, umzubenennen oder zu modifizieren. Auch ohne diese Berechtigung können Benutzer Abfragen ausführen, die automatisch benutzerdefinierte Spalten erstellen.
Remove custom column	Ermöglicht es den Benutzern, eine benutzerdefinierte Spalte in der „Results Table“ zu löschen.
Modify Results Table column settings	Ermöglicht es den Benutzern, Spalteneinstellungen der „Results Table“ in einer „Results Table“ zu ändern.
Save Column Settings as Project Default	Ermöglicht es den Benutzern, die Spalteneinstellungen auf das Projekt anzuwenden.
Lock and save Results Table	Ermöglicht es den Benutzern, eine „Results Table“ zu sperren und zu speichern.
Unlock and save Results Table	Ermöglicht es den Benutzern, eine „Results Table“ zu entsperren und zu speichern.
Review and save Results Table	Ermöglicht es den Benutzern, die „Results Table“ zu überprüfen und zu speichern.

Voreinstellung Zugriff	Beschreibung
Create or edit queries in Results Tables	Ermöglicht den Benutzern das Erstellen oder Bearbeiten von Abfragen in einer „Results Table“ mithilfe einer der folgenden Optionen: • Klicken Sie auf **Process** > **Create Simple Query**. • Klicken Sie auf **Process** > **Edit Simple Query**.
Use Results Table queries	Ermöglicht es Benutzern, Abfragen auszuführen. (Klicken Sie auf **Process** > **Query**.)
Use unencrypted MultiQuant queries	Ermöglicht es Benutzern, .xls-Abfragen von dem MQ Settings-Ordner aus auszuführen.

Hinweis: Wenn die MultiQuant MD Software deinstalliert wird, dann verbleiben die MultiQuant MD Software-Sicherheitselemente in der Analyst MD Software. Sicherheitselemente finden Sie auf der Registerkarte „Roles“ im Dialogfeld „Security Configuration“.

Einen Benutzer oder eine Gruppe in der Analyst MD Software hinzufügen

Hinweis: Änderungen der Analyst MD-Software-Sicherheitskonfiguration werden nach dem Neustart der Analyst MD-Software wirksam.

1. Doppelklicken Sie in der Navigationsleiste unter **Configure** auf **Security Configuration**.
   Das Dialogfeld „Security Configuration“ wird geöffnet.
2. Öffnen Sie die Registerkarte „People“.
3. Klicken Sie auf **New Person**.
   Das Dialogfeld „Select Users or Groups“ wird geöffnet.
4. Fügen Sie einen Benutzer oder eine Gruppe hinzu.
5. Klicken Sie im Teilfenster „Available Roles“ auf eine Rolle und klicken dann auf **Add**.
6. Klicken Sie auf **Apply**.
7. Klicken Sie auf **OK**.
   Das Dialogfeld „Select Users or Groups“ wird geschlossen.
8. Klicken Sie auf **OK**.
   Das Dialogfeld „Security Configuration“ wird geschlossen.

Ändern einer Rolle

1. Doppelklicken Sie in der Navigationsleiste unter **Configure** auf **Security Configuration**.
   Das Dialogfeld „Security Configuration“ wird geöffnet.

2. Öffnen Sie die Registerkarte „People“.
3. Im linken Fensterbereich klicken Sie auf die Person und führen dann einen der folgenden Schritte durch:
   - Im Bereich „Available Roles“ klicken Sie auf die gewünschte Rolle und klicken dann auf **Add**, um die Rolle hinzuzufügen.
   - Im Bereich „Role(s) Selected“ klicken Sie auf die gewünschte Rolle und klicken dann auf **Remove**, um die Rolle zu entfernen.
4. Klicken Sie auf **Apply**.
5. Klicken Sie auf **OK**.
   Das Dialogfeld „Security Configuration“ wird geschlossen.

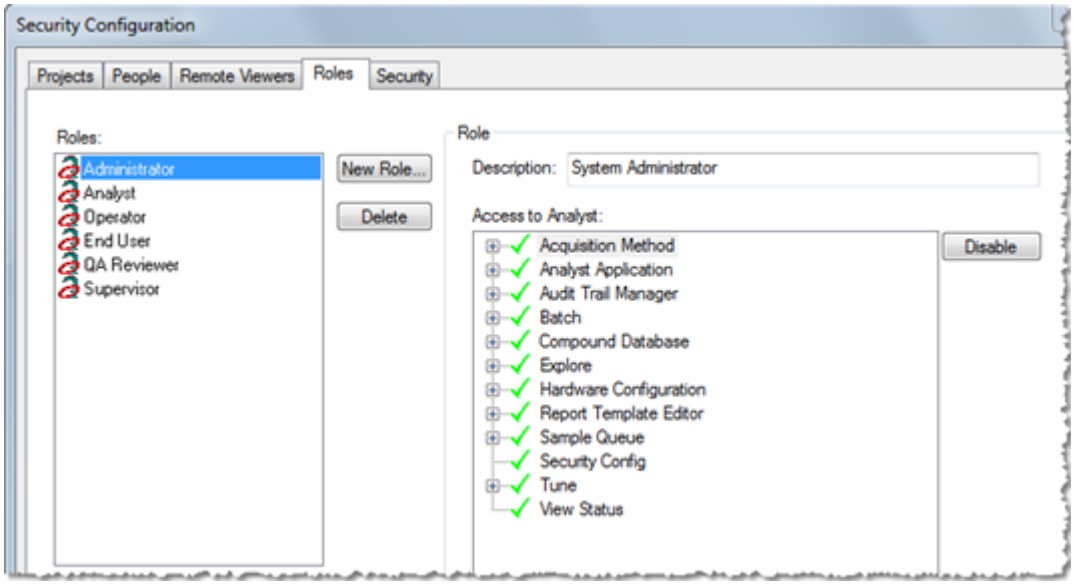
Personen von der Analyst MD Software entfernen

1. Doppelklicken Sie in der Navigationsleiste unter **Configure** auf **Security Configuration**.
   Das Dialogfeld „Security Configuration“ wird geöffnet.
2. Öffnen Sie die Registerkarte „People“.
3. Im linken Fensterbereich klicken Sie auf die zu entfernende Person und klicken dann auf **Delete**.
4. Klicken Sie auf **Apply**.
5. Klicken Sie auf **OK**.
   Das Dialogfeld „Security Configuration“ wird geschlossen.

Erstellen einer benutzerdefinierten Rolle

1. Doppelklicken Sie in der Navigationsleiste unter **Configure** auf **Security Configuration**.
   Das Dialogfeld „Security Configuration“ wird geöffnet.
2. Klicken Sie auf **More** und öffnen Sie dann die Registerkarte „Roles“.

Abbildung 5-6: Dialog „Security Configuration“: Registerkarte „Roles“



3. Klicken Sie auf **New Role**.
   Das Dialogfeld „New Role“ wird geöffnet.
4. Geben Sie den **Role Name** und die **Description** in die entsprechenden Felder ein.
5. Klicken Sie auf **OK**.

Hinweis: Alle neuen benutzerdefinierten Rollen haben vollen Zugriff auf die Analyst MD Software. Im Teilfenster „Access to Analyst“ zeigt ein grünes Häkchen, dass der Systemzugriff aktiviert ist. Ein rotes X zeigt, dass der Systemzugriff verweigert wird.

6. Doppelklicken Sie auf die Komponenten in der Liste **Access to Analyst**, um den Zugriff zu aktivieren oder zu deaktivieren.
7. Um den Zugriff auf funktionaler Ebene zu konfigurieren, erweitern Sie die Komponenten und doppelklicken dann auf die Funktionalität, um diese zu aktivieren oder zu deaktivieren.
8. Klicken Sie auf **Apply**.
9. Klicken Sie auf **OK**.
   Das Dialogfeld „Security Configuration“ wird geschlossen.

Löschen einer benutzerdefinierten Rolle

Hinweis: Wenn eine Person einer einzigen Rolle zugeordnet ist und diese Rolle gelöscht werden soll, werden Sie aufgefordert, sowohl die Person als auch die Rolle zu löschen.

1. Doppelklicken Sie in der Navigationsleiste unter **Configure** auf **Security Configuration**.
   Das Dialogfeld „Security Configuration“ wird geöffnet.
2. Klicken Sie auf **More** und öffnen Sie dann die Registerkarte „Roles“.
   Das Teilfenster „Roles“ wird geöffnet.

3. Wählen Sie die Rolle aus und klicken Sie auf **Delete**.
4. Klicken Sie auf **Apply**.
5. Klicken Sie auf **OK**.
   Das Dialogfeld „Security Configuration“ wird geschlossen.

Zugriff festlegen

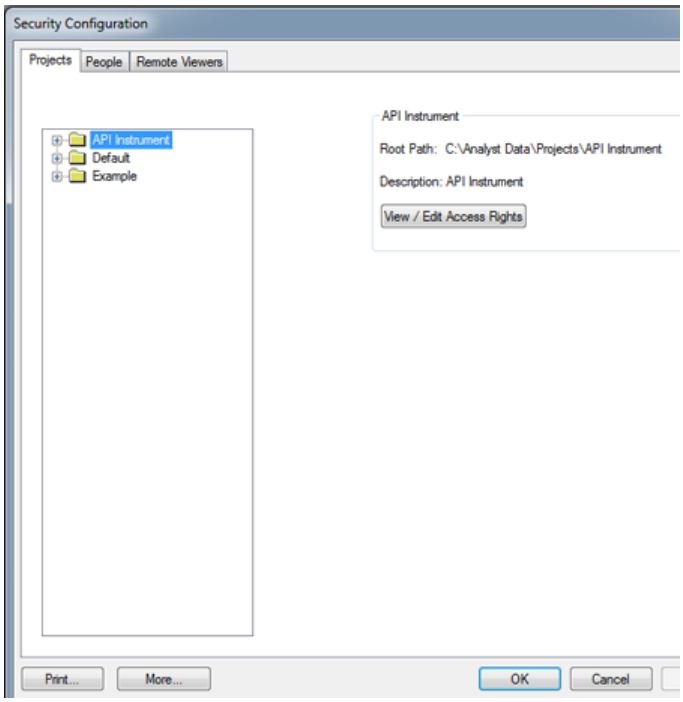
Ein Administrator kann den Zugriff auf Projekte und Projektdateien nach Personen oder Gruppen konfigurieren und den Zugriff nach Personen oder mithilfe der Windows-Sicherheitsgruppen steuern.

Um diese Funktion der Analyst MD-Softwaresicherheit zu nutzen, verwenden Sie NTFS für den Betrieb. Wenn der Administrator keine Projektsicherheit festlegt, hängt der Operator-Zugriff auf die Projektdateien von den Daten ab, die für die einzelnen Windows-Benutzer in NTFS eingestellt wurden. Weitere Informationen finden Sie im Abschnitt: Windows-Sicherheitskonfiguration.

Hinweis: Wenn ein Projekt mit der Analyst MD-Software erstellt wird, haben alle Benutzer Zugriff auf die Projektordner und Unterordner.

1. Doppelklicken Sie in der Navigationsleiste unter **Configure** auf **Security Configuration**.

   Abbildung 5-7: Dialogfeld „Security Configuration“: Registerkarte „Projects“



2. Klicken Sie im linken Fensterbereich auf einen Ordner oder eine Datei.
3. Klicken Sie auf **View/Edit Access Rights**.
   Das Dialogfeld „Properties“ wird geöffnet.

4. Fügen Sie Benutzer oder Gruppen hinzu oder entfernen Sie diese, und legen Sie nach Bedarf Berechtigungen fest und klicken Sie anschließend auf **OK**.
5. Klicken Sie auf **Apply**.
6. Klicken Sie auf **OK**.
   Das Dialogfeld „Select Users or Groups“ wird geschlossen.
7. Klicken Sie auf **OK**.
   Das Dialogfeld „Security Configuration“ wird geschlossen.

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 5-16.

Tabelle 5-16: Projektordner

Ordner	Inhalt
\Acquisition Methods	Enthält alle verwendeten Erfassungsmethoden. Erfassungsmethoden haben die Erweiterung .dam.
`\Acquisition Scripts`	Erfassungsskripte sind in der Analyst MD-Software nicht verfügbar. Dieser Ordner ist leer. Das Analyst MD „Software Scripting“, mit dem benutzerdefinierte Skripte (benutzerdefinierte Sequenzen für den Analyst-Betrieb) erstellt werden können, sollte nicht als Teil eines *In-Vitro*-Diagnostik-Systems verwendet werden. Inhärente Software-Prüfungen, die bei der Arbeit mit der Analyst MD Software durchgeführt werden, werden bei benutzerdefinierten Scripts nicht ausgeführt und können zu Problemen führen.
`\Batch`	Enthält alle Erfassungschargendateien, die gespeichert wurden. Erfassungschargen haben die Erweiterung .dab. Dieser Ordner enthält außerdem einen Unterordner namens „`Templates`“ mit Erfassungschargen-Vorlagen. Chargen-Vorlagen haben die Erweiterung .dat.
`\Data`	Enthält die Dateien mit den Erfassungsdaten. Diese Dateien haben die Erweiterung .wiff.
`\Log`	Enthält die Ergebnisse von Quantifizierungen und Verbindungsoptimierungen.
`\Processing Methods`	Enthält alle verwendeten qualitativen Datenverarbeitungsmethoden.
`\Processing Scripts`	Enthält zwei Datenverarbeitungs-Skripte. Im „`API Instrument`“-Projekt gespeicherte Verarbeitungsskripte werden im Menü „**Scripts**“ angezeigt.
`\Project Information`	Enthält alle Projektinformationen und Einstellungen für das Projekt. Dieser Ordner kann nicht in einem Teilprojekt gespeichert werden.

Tabelle 5-16: Projektordner (Fortsetzung)

Ordner	Inhalt
`\Quantitation Methods`	Enthält alle verwendeten Quantifizierungsmethoden. Quantifizierungsmethoden haben die Erweiterung .qmf.
`\Results`	Enthält alle Quantifizierungs-„Results Tables“ (.rdb-Erweiterung).
`\Templates`	Enthält Berichtsvorlagen (.rpt-Erweiterung)

Software-Dateitypen

Für gängige Dateitypen der Analyst MD-Software siehe die Tabelle: Tabelle 5-17. Der Ordner „`API Instrument`“ enthält alle Unterverzeichnisse außer „`Processing Methods`“ und „`Results`“.

Tabelle 5-17: Analyst MD-Softwaredateien

Erweiterung	Dateityp	Ordner
ata	Audit-Trail-Archive	`Project Information`
atd	• Daten des Geräte-Audit-Trails • Einstellungen des Geräte-Audit-Trails • Daten des Projekt-Audit-Trails • Einstellungen des Projekt-Audit-Trails	Project Information
cam	Audit-Map	`Project Information`
dab	Erfassungscharge	`Batch`
dam	Erfassungsmethode	`Acquisition Methods`
dat	Erfassungschargen-Vorlage	`Batch\Templates`
dll	Dynamic Link Library	`Processing Scripts`
eph	Daten zur Verarbeitungshistorie	`Processing Methods`
hwpf	Hardwareprofil	`Configuration`[3]
ins	Informationen zur Gerätedatenkalibrierung	`Instrument Data`[3]
log	Protokollsätze aus automatisierten Sammlungen	`Log`

[3] Existiert nur im API Instrument-Ordner. Alle anderen Unterordner sind in jedem Projektordner vorhanden. Sie können sich im Ordner auf Projektebene oder in jedem Teilprojekt befinden.

Tabelle 5-17: Analyst MD-Softwaredateien (Fortsetzung)

Erweiterung	Dateityp	Ordner
mdb	MS Access-Datenbank	—
pdf	Daten im PDF-Format	—
psf	Parametereinstellungen	`Parameter Settings`[3]
qmf	Quantifizierungsmethode	`Quantitation Methods`
rdb	Results Table. Enthält Audit-Trail-Daten für die Quantifizierung	`Results`
rpt	Berichtsvorlage	• `Templates\Batch` • `Templates\Method` • `Templates\ Report` • `Templates\Workspace`
rtf	Rich Text Format	—
sdb	Einstellungen des Audit-Trails für die Quantifizierung	`Project Information`
tun	Tuning-Präferenz-Datei	`Preferences`[3]
txt	Text	—
wiff.scan	Datei mit Massenspektrometriedaten	• `Tuning` Cache[3] • `Data`
xls oder xlsx	Excel-Tabelle	`Batch`

Im `Example`-Projekt werden die folgenden Formate für den Import von Chargeninformationen unterstützt:

- mdb
- txt
- xls oder xlsx

Konfiguration der Windows-Firewall auf dem Erfassungs- und dem Clientcomputer

Um ein Massenspektrometer mit der Analyst MD Software auf einem Clientcomputer dezentral zu verwalten, müssen Sie die Windows-Firewall sowohl auf dem Erfassungscomputer als auch auf den Clientcomputern konfigurieren. Windows-Firewall muss auf dem Erfassungscomputer so konfiguriert sein, dass sowohl Analyst.exe als auch AnalystService.exe ausgeführt werden können. Auf dem Clientcomputer muss Windows-Firewall so konfiguriert sein, dass Analyst.exe ausgeführt werden kann.

Hinweis: Sowohl der Erfassungscomputer, auf den aus der Ferne zugegriffen wird, als auch der Clientcomputer, von dem auf den Erfassungscomputer zugegriffen wird, sollten sich auf derselben Netzwerkdomäne befinden.

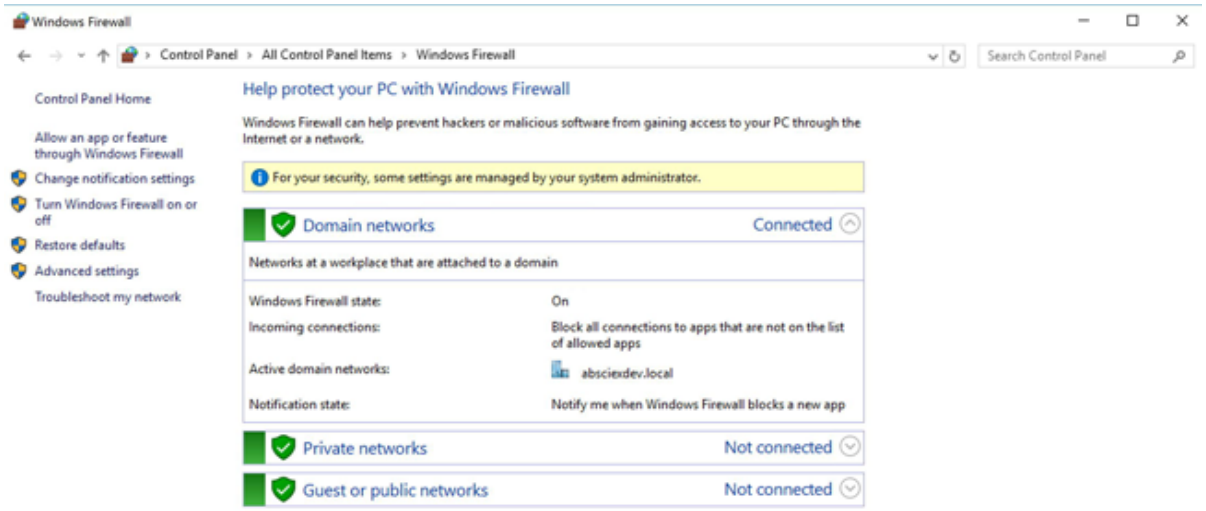
Hinweis: Stellen Sie auf dem Erfassungscomputer sicher, dass nach Übermittlung einer Charge die Seite der Warteschlange geöffnet bleibt, damit diese Warteschlange über den Clientcomputer aus der Ferne angezeigt werden kann.

Konfigurieren der Windows Firewall auf dem Erfassungscomputer

Der Erfassungscomputer muss so eingestellt sein, dass seine Firewall Analyst.exe und AnalystService.exe nicht blockiert.

1. Öffnen Sie das „Control Panel“ und dann die Windows Firewall.

   Abbildung 5-8: Control Panel



2. Klicken Sie im linken Teilfenster auf **Allow an app or feature through Windows Firewall**.
3. Klicken Sie auf **Change Settings.**.
4. Klicken Sie auf **Allow another app**.
   Das Dialogfeld Add an app wird geöffnet.
5. Klicken Sie auf **Browse** und navigieren Sie zum Ordner `C:\Program Files(x86)\Analyst\bin`.
6. Klicken Sie auf **AnalystService.exe** und dann auf **Open**.
7. Klicken Sie auf **Add**.
   Der AnalystService wird der Liste **Allowed apps and features** hinzugefügt.
8. Wenn **AB SCIEX Analyst** noch nicht in der Liste **Allowed apps and features** enthalten ist, dann fügen Sie **Analyst.exe** hinzu, indem Sie die Schritte 3 bis wiederholen. Hierbei wählen Sie jedoch nicht AnalystService.exe aus, sondern **Analyst.exe** in Schritt 6.

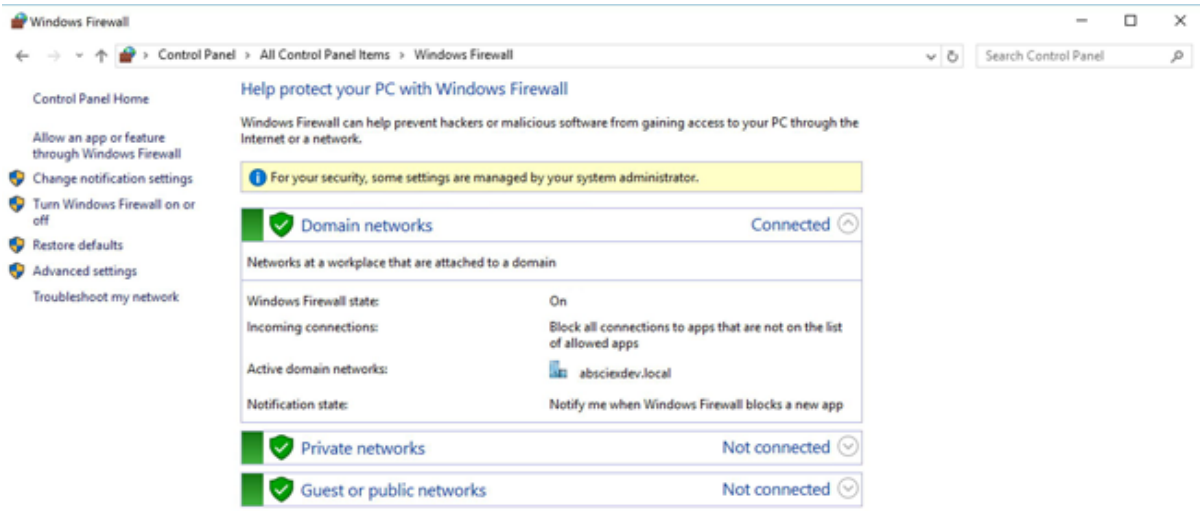
9. Klicken Sie auf **OK**.

Konfigurieren der Windows-Firewall auf dem Client-Computer

Wenn Analyst.exe nicht in der Liste der zulässigen Anwendungen und Merkmale für die Windows-Firewall auf dem Client-Computer enthalten ist, fügen Sie sie hinzu.

1. Öffnen Sie das „Control Panel“ und dann die Windows Firewall.

Abbildung 5-9: Control Panel



2. Klicken Sie im linken Teilfenster auf **Allow an app or feature through Windows Firewall**.
3. Klicken Sie auf **Change Settings.**.
4. Klicken Sie auf **Allow another app**.
   Das Dialogfeld Add an app wird geöffnet.
5. Klicken Sie auf **Browse** und navigieren Sie zum Ordner `C:\Program Files(x86)\Analyst\bin`.
6. Klicken Sie auf **Analyst.exe** und dann auf **Open**.
7. Klicken Sie auf **Add**.
   AB SCIEX Analyst wird der Liste **Allowed apps and features** hinzugefügt.
8. Klicken Sie auf **OK**.

Remote-Workstations

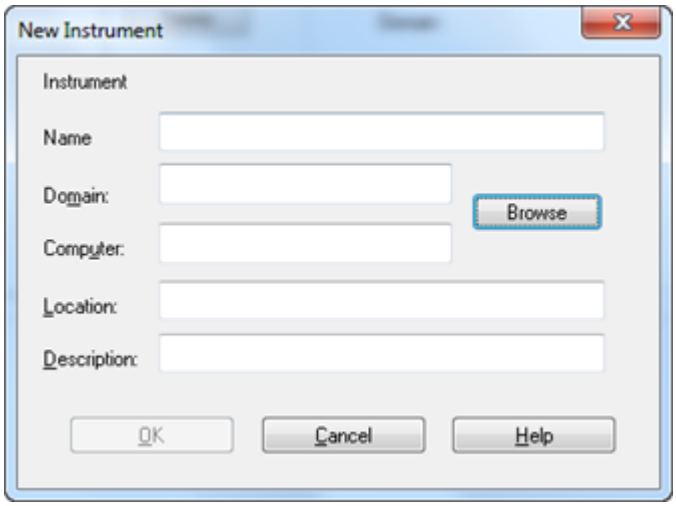
Auf einem lokalen Computer kann eine Liste von Massenspektrometern eingerichtet werden. Dann können die Probenwarteschlangen dieser Massenspektrometer aus der Ferne überwacht werden. Benutzer können nur die Proben-Warteschlange und den Status der Massenspektrometer auf diesen Remote-Arbeitsplätzen einsehen. Selbst wenn sie andere Aktionen am lokalen Arbeitsplatz ausführen können, können sie diese auf einem fernen Arbeitsplatzrechner nicht durchführen.

Hinweis: Sowohl der Erfassungscomputer, auf den aus der Ferne zugegriffen wird, als auch die lokale Workstation, von der aus auf den Erfassungscomputer zugegriffen wird, sollten sich auf derselben Netzwerkdomäne befinden.

Hinzufügen des Zugriffs auf eine Workstation

1. Melden Sie sich bei der Analyst MD Software als domänenbasierter Benutzer (user@domain) an.
2. Doppelklicken Sie in der Navigationsleiste unter **Configure** auf **Security Configuration**. Das Dialogfeld „Security Configuration“ wird geöffnet.
3. Öffnen Sie die Registerkarte „Waters Empower“ und klicken Sie dann auf **Add**.

Abbildung 5-10: Dialogfeld „New Instrument“



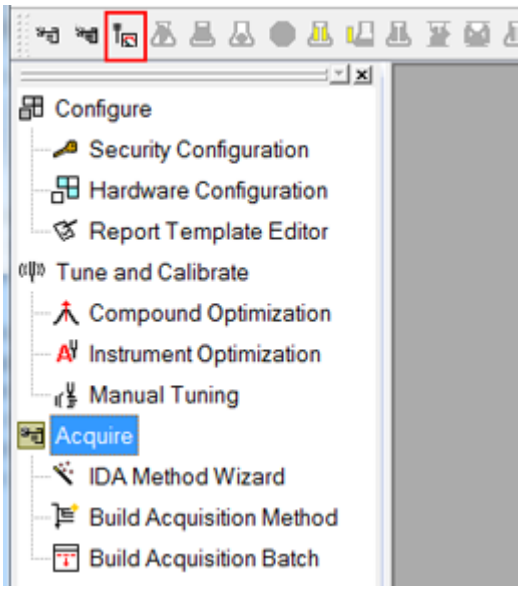
4. Geben Sie den Namen der Workstation in das Feld **Name** ein.
   Wenn „Active Directory“ in der systemeigenen Umgebung verwendet wird, ist das Feld „Domain“ nicht sichtbar und ein Benutzername kann im UPN-Format eingegeben werden.
5. Falls erforderlich, geben Sie Ortsinformationen in das Feld **Location** ein.
6. Klicken Sie auf **Browse**, um zu einer **Domain** und einem **Computer** zu navigieren. Das Dialogfeld „Select Computers“ wird geöffnet.
7. Wählen Sie ein Massenspektrometer aus, indem Sie auf **Object Types** klicken. Das Dialogfeld „Windows Security“ wird geöffnet.
8. Geben Sie die Zugangsdaten der Domäne ein und klicken Sie dann auf **OK**. Das Dialogfeld „Select Computers“ wird angezeigt.
9. Klicken Sie auf **Locations**.
   Das Dialogfeld „Locations“ wird geöffnet.
10. Klicken Sie auf das Netzwerk, in dem sich der dezentrale Erfassungscomputer befindet, und dann auf **OK**.
    Das Dialogfeld „Select Computers“ wird angezeigt.

11. Geben Sie den Namen des Erfassungscomputers im Feld **Enter the object names to select** ein.
12. Klicken Sie auf **Check Names**.
13. Klicken Sie auf **OK**.
14. Geben Sie gegebenenfalls im Feld **Description** im Dialogfeld „New Instrument“ eine Beschreibung ein.
15. Klicken Sie auf **OK**.
    Der Name des Erfassungscomputers und der Domäne werden auf der Registerkarte „Remote Viewers“ angezeigt.
16. Klicken Sie auf **Apply**.
17. Klicken Sie auf **OK**.
    Das Dialogfeld „Security Configuration“ wird geschlossen.
18. Starten Sie die Analyst MD Software neu.

Ansehen des Status des Ferninstruments und der Warteschlange der Probenerfassung

Um auf dem Erfassungscomputer den Status des Instruments und der angeschlossenen Geräte sowie die Warteschlange einer Probenerfassung aus der Ferne anzusehen, verwenden Sie das Symbol **Status for Remote Instrument** in der Analyst MD Software auf dem Client-Computer.

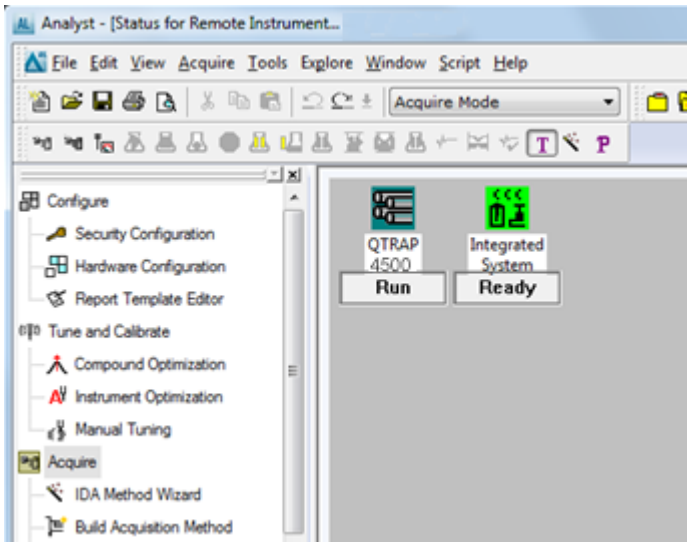
Abbildung 5-11: Symbol „Status for Remote Instrument“ in der Analyst MD Software



1. Melden Sie sich bei der Analyst MD Software als derselbe domänenbasierte Benutzer an, der verwendet wurde, um das Ferninstrument im Dialogfeld „Security Configuration“ in Hinzufügen des Zugriffs auf eine Workstation hinzuzufügen.

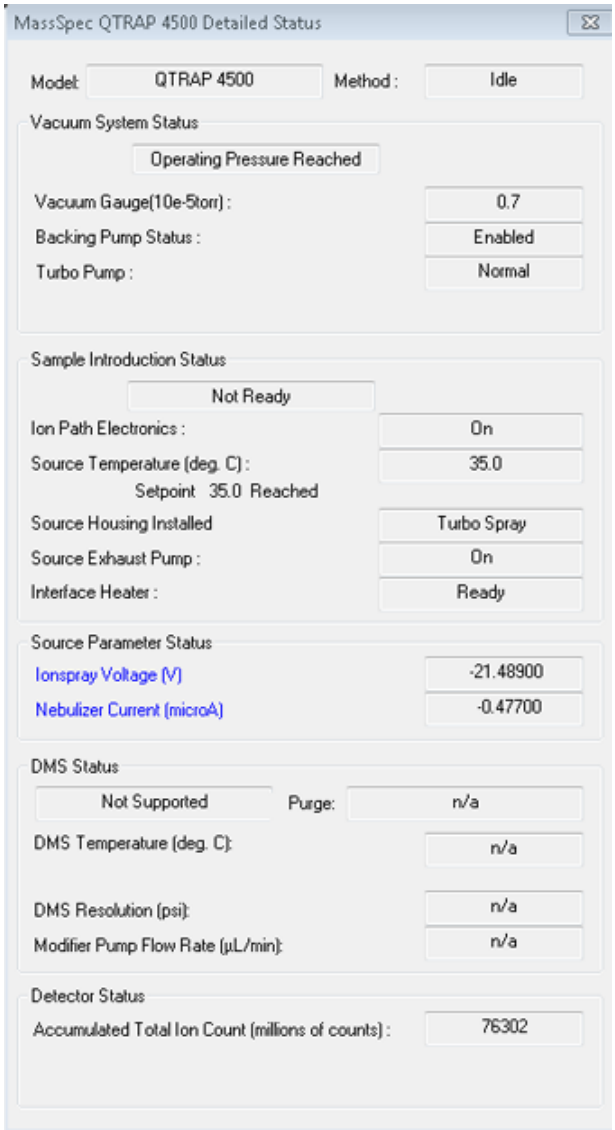
2. Klicken Sie in der Analyst MD Software auf dem Client-Computer bei ausgewähltem **Acquire**-Modus auf das Symbol **Status for Remote Instrument**.
3. Wählen Sie im Dialogfeld „Remote Instrument Station“ das Instrument im Feld **Select the Instrument Station** und klicken Sie dann auf **Connect**.

Abbildung 5-12: „Remote Instrument Station“ und „Integrated Device“ wird in der Analyst MD Software angezeigt



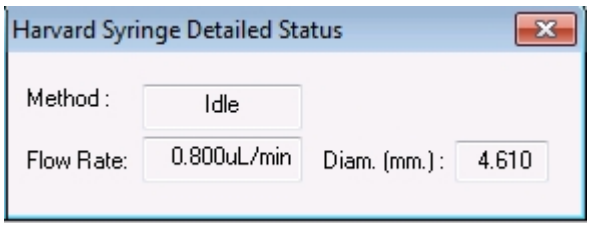
4. Doppelklicken Sie zur detaillierten Statusansicht auf das Symbol des Ferninstruments.

Abbildung 5-13: Detaillierter Status des Ferninstruments



5. Doppelklicken Sie zur detaillierten Statusansicht auf das Symbol der integrierten Spritze.

Abbildung 5-14: Detaillierter Status der integrierten Spritze

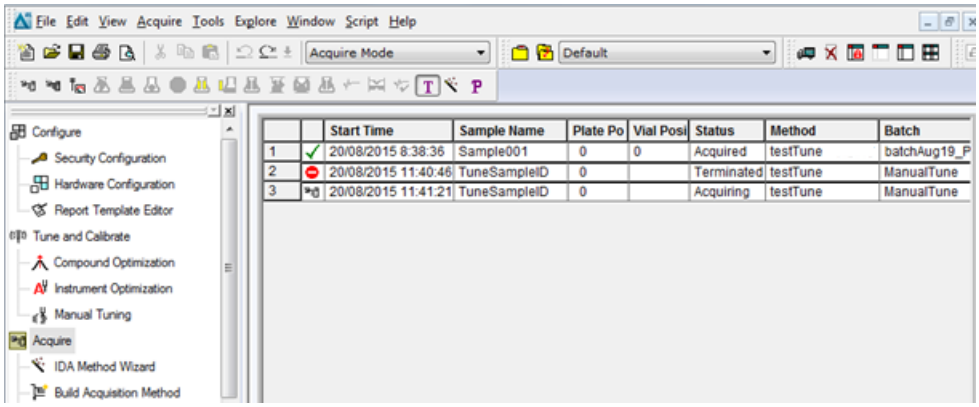


6. Zum Anzeigen der Warteschlange der Probenerfassung auf dem Erfassungscomputer klicken Sie im Modus **Acquire** auf das Symbol **Instrument Queue** in der Symbolleiste der Analyst MD Software.

Hinweis: Die Seite der Warteschlange auf dem Erfassungscomputer muss geöffnet bleiben, damit diese Warteschlange über den Clientcomputer aus der Ferne angezeigt werden kann.

7. Wählen Sie im Dialog „Remote Instrument Station“ das Instrument im Kontrollkästchen **Select the Instrument Station** und klicken Sie dann auf **Connect**.
   Die Warteschlange der Probenerfassung auf dem Erfassungscomputer wird in der Analyst MD Software angezeigt.

   Abbildung 5-15: Warteschlange einer Probenerfassung auf dem Erfassungscomputer



Zugriff auf eine Workstation entfernen

1. Doppelklicken Sie in der Navigationsleiste unter **Configure** auf **Security Configuration**.
2. Öffnen Sie im Dialogfeld „Security Configuration“ die Registerkarte „Remote Viewers“.
3. Im linken Fensterbereich wählen Sie einen Computer aus.
4. Klicken Sie auf **Delete**.
5. Klicken Sie zum Bestätigen auf **Yes**.
6. Klicken Sie auf **OK**, um das Dialogfeld Security Configuration zu schließen.
7. Starten Sie die Analyst MD Software neu.

Drucken der Sicherheitskonfigurationen

Drucken Sie eine Kopie der Sicherheitskonfigurationen als Nachweis in Ihren Akten.

1. Doppelklicken Sie in der Navigationsleiste unter **Configure** auf **Security Configuration**.
   Das Dialogfeld „Security Configuration“ wird geöffnet.
2. Klicken Sie auf **Print**.
3. Klicken Sie auf **Apply**.
4. Klicken Sie auf **OK**.
   Das Dialogfeld „Security Configuration“ wird geschlossen.

Überwachung des Systemstatus 6

Zusätzliche Kurven

Die zusätzlichen Kurven für ein LC-System wie z. B. die Pumpen-Druckkurve und die Säulenofen-Temperaturkurve können in der Datendatei für jede Probe gespeichert werden. Diese Kurven können für die Überwachung der Integrität eines LC-Systems verwendet werden. Die Kurven, insbesondere die Pumpen-Druckkurve, können dabei helfen, LC-bezogene Probleme zu behandeln.

Die Funktion für zusätzliche Kurven wird in der Analyst MD Software ab Version 1.7.3 unterstützt.

Zusätzliche Kurven aktivieren

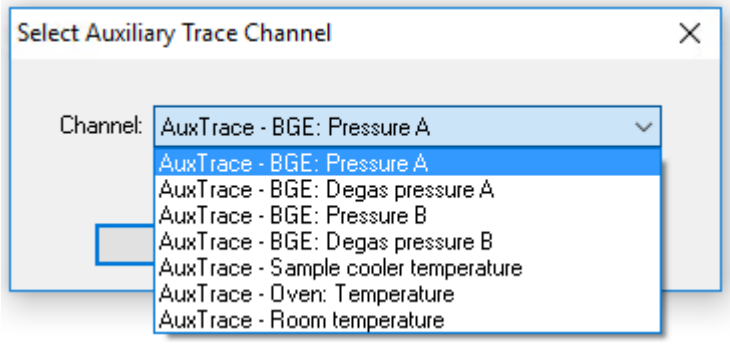
Um die Funktion für zusätzliche Kurven zu aktivieren, befolgen Sie die folgenden Schritte bei Konfigurieren des LC-Geräts im Hardwareprofil.

1. Wählen Sie im Dialogfeld „Create New Hardware Profile“ oder „Edit Hardware Profile“ das LC-System aus und klicken Sie dann auf **Setup Device**.
2. Aktivieren Sie das Kontrollkästchen **Enable Aux Trace Monitoring**.
3. Stellen Sie sicher, dass die Konfiguration des LC-Systems abgeschlossen ist und klicken Sie dann auf **OK**.
4. Aktivieren Sie das Hardwareprofil.
5. Erfassen von Daten.

Zusätzliche Kurven anzeigen

1. Stellen Sie sicher, dass der richtige Projektordner ausgewählt wird.
2. Doppelklicken Sie in der Navigationsleiste unter **Explore** auf **Open Data File**.
   Das Dialogfeld „Select Sample“ wird geöffnet.
3. Klicken Sie im Feld **Data Files** auf die Datendatei, die erfasst wurde, nachdem die Überwachung zusätzlicher Kurven aktiviert wurde.
4. In der **Samples**-Liste wählen Sie eine Probe und klicken Sie dann auf **OK**.
5. Klicken Sie auf **Explore** > **Show** > **Show Auxiliary Traces**.

Abbildung 6-1: Dialogfeld „Select Auxiliary Trace Channel“



6. Wählen Sie einen Kanal in der **Channel**-Liste aus und klicken Sie dann auf **OK**.
   Die ausgewählte zusätzliche Kurve wird in einem neuen Teilfenster unterhalb des aktiven Teilfensters angezeigt.

Injektionszähler

Mithilfe des Injektionszählers kann der Benutzer die Anzahl der Probeninjektionen auf einer bestimmten Analysesäule auf einem einzeln übertragenden LC-MS/MS-System überwachen. Diese Funktion hilft dem Benutzer dabei, den Zeitpunkt eines Säulenwechsels zu bestimmen, um eine erneute Ausführung der Charge zu vermeiden.

Den Injektionszähler aktivieren

1. Stellen Sie sicher, dass sich das System im Standby-Zustand befindet.
2. Klicken Sie im Modus **Configure** auf **Tools** > **Settings** > **Injection Counter Options**.
3. Aktivieren Sie das Kontrollkästchen **Enable Injection Counter**.
4. Vervollständigen Sie eine Zeile für jede Analyse-Spalte, in der Injektionen gezählt werden.
   Jede Zeile enthält die Felder in der folgenden Tabelle.

Tabelle 6-1: Dialogfelder „Injection Counter“

Feld	Beschreibung
Active	Wählen Sie diese Option aus, um die Injektionszählung für diese Analysesäule zu aktivieren. Wenn diese Option ausgewählt ist, wird die Anzahl der Injektionen auf dieser Analysesäule für jede Injektion um Eins inkrementiert. Wenn der Säulenwechsel verwendet wird, können mehrere Analysesäulen gleichzeitig aktiv sein.
Column Description	Geben Sie Informationen ein, um die Säule in Berichten und Anzeigen zu identifizieren. Nehmen Sie Informationen wie z. B. Marke, Typ, Partikelgröße, Säulendurchmesser und Säulenlänge auf.
Column S/N	Geben Sie die Seriennummer der Analysesäule ein.

Tabelle 6-1: Dialogfelder „Injection Counter“ (Fortsetzung)

Feld	Beschreibung
Number of injections	Geben Sie beim Konfigurieren der Einstellungen für den Injektionszähler die Anzahl der Injektionen ein, die auf der Analysesäule bereits erfolgt sind. Wenn die Injektionszähler-Funktion aktiviert ist, dann inkrementiert die Software dieses Feld automatisch während des Betriebs eines LC-Systems mit Autosampler.
Threshold	Geben Sie die Anzahl der Injektionen ein, bei der eine Warnung ausgelöst wird. Wenn der Benutzer eine Charge übergibt, die dazu führt, dass die Anzahl der Injektionen diesen Schwellenwert übersteigt, dann wird eine Warnung angezeigt. Der Benutzer kann dann fortfahren, oder die Charge abbrechen und eine andere Analysesäule verwenden. Verschiedene aktive Analysesäulen können unterschiedliche Schwellenwerte aufweisen. **Hinweis:** Stellen Sie sicher, dass Sie die Injektionszähler-Einstellungen aktualisieren, nachdem eine andere Säule installiert wurde.

5. Um zusätzliche Analysesäulen hinzuzufügen, klicken Sie auf **+** und wiederholen Sie dann Schritt 4.

Hinweis: Um eine Analysesäule aus der Liste zu entfernen, klicken Sie auf das Minus-Zeichen (**-**) rechts von der Säule.

6. 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 Analyst MD Software unterteilt überwachte Ereignisse basierend auf dem Massenspektrometer, Projekt oder der Quantifizierung in verschiedene Audit-Trails. Hierbei handelt es sich um Dateien, die Aufzeichnungen von überwachten Ereignissen speichern. Audit-Trails bilden in Verbindung mit Dateien, wie z. B. .wiff-Dateien und „Results Table“-Dateien, gültige elektronische Aufzeichnungen, die für Compliance-Zwecke verwendet werden können.

Tabelle 7-1: Analyst MD-Software-Audit-Trails-Audit-Trails

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

Gerät (eines pro Workstation)	• Änderungen an:
	  • Geräte-Auflösungen
	  • Massenkalibrierungen
	  • Probenwarteschlangen
	  • Sicherheit
	  • Hardwareprofile
	• Einträge in Geräte-Wartungsprotokollen
		• `API Instrument` Projekt
		• Ordner `Project Information`
			• Bei Neuinstallation, Standard-Audit-Map

Tabelle 7-1: Analyst MD-Software-Audit-Trails-Audit-Trails (Fortsetzung)

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

Projekt (1x pro Projekt)	• Änderungen an:
	  • Projekt
	  • Methode
	  • Quantifizierung
	  • Charge
	  • Daten
	  • Results Table
	  • Tuning
	  • Berichtvorla-gendateien
	• Öffnen und Schließen von Modulen
	• Drucken
		• Jedes Projekt
		• Ordner `Project Information`
			• Kopiert aus dem Standard-Projekt

Quantifizierung (1x pro „Results Table“)	Änderungen an: • Quantifizierungs-methoden • Probeninforma-tionen • Peak-Integrationspara-meter	• „Results Table“-Datei (rdb-Datei)	• Kopiert aus dem übergeordneten Projekt

Sobald der Geräte-Audit-Trail oder Projekt-Audit-Trail 1000 Audit-Aufzeichnungen enthält, archiviert die Analyst MD-Software diese Aufzeichnungen automatisch und beginnt einen neuen Audit-Trail. Weitere Informationen finden Sie im Abschnitt: Audit-Trail-Aufzeichnungen.

Audit-Maps

Audit-Maps sind Dateien und legen Folgendes fest:

- Ereignisse, die überwacht werden

- Überwachte Ereignisse, bei denen der Bediener die Gründe für die Änderung angeben muss
- Überwachte Ereignisse, die elektronische Signaturen erfordern

Für das Massenspektrometer und für Projekte können viele Audit-Maps erstellt werden. Es kann jedoch immer nur jeweils eine Audit-Map pro Erfassungscomputer und Projekt verwendet werden. Die verwendete Audit-Map wird als die aktive Audit-Map für dieses Massenspektrometer oder Projekt bezeichnet.

Audit-Maps enthalten eine Liste aller Ereignisse, die überwacht werden können. Je nachdem, wo diese Map verwendet wird, gelten diese Ereignisse für den Geräte-Audit-Trail oder die Projekt- und Quantifizierungs-Audit-Trails. Geben Sie für jedes Ereignis an, ob es geprüft wird oder eine elektronische Signatur erforderlich ist, und legen Sie bis zu zehn vordefinierte Gründe für das Ereignis fest.

Wenn der Benutzer ein neues Projekt erstellt, werden die Audit-Maps für das Projekt aus dem `Default`-Projekt kopiert. Die aktive Audit-Map im Standardprojekt wird die aktive Audit-Map im neuen Projekt.

Wenn der Benutzer eine neue „Results Table“ erstellt, wird die Konfiguration des Quantifizierungs-Audit-Trails durch die Quantifizierungsereignisse in der aktiven Audit-Map für das Projekt definiert. Beim Speichern einer „Results Table“ wird die Audit-Konfiguration aus der aktiven Audit-Map permanent mit der „Results Table“ gespeichert. Wenn die aktive Audit-Map (bezogen auf das Projekt) geändert wird, bleibt die ursprüngliche Audit-Konfiguration in der „Results Table“-Datei eingebettet. Die eingebettete Konfiguration kann von der veränderten Audit-Map am Datum und der Uhrzeit der letzten Änderungen unterschieden werden, die auf der Registerkarte „Settings“ angezeigt wird.

Einrichten von Audit-Maps

Bevor Sie mit zu auditierenden Projekten arbeiten können, müssen Sie den Standardarbeitsanweisungen entsprechende Audit-Maps konfigurieren. Bei der Installation der Analyst MD-Software liegen bereits mehrere standardmäßige Audit-Maps vor, von denen eine oder mehrere benutzerspezifisch angepasst werden können. Stellen Sie sicher, dass Sie eine geeignete Audit-Map für den Geräte-Audit-Trail und eine geeignete Audit-Map für jedes Projekt haben.

Tabelle 7-2: Checkliste für das Konfigurieren von Auditing

Aufgabe	Siehe
Erstellen einer Audit-Map für den Geräte-Audit-Trail	• Erstellen einer Audit Map. • Ändern einer Audit Map.
Anwendung der Audit-Map auf den Geräte-Audit-Trail	• Anwenden einer Audit Map.
Erstellen einer standardmäßig aktiven Audit-Map für neue Projekte	• Erstellen einer Audit Map. • Ändern einer Audit Map.

Tabelle 7-2: Checkliste für das Konfigurieren von Auditing (Fortsetzung)

Aufgabe	Siehe
Spezifizierung der standardmäßig aktiven Audit-Map für neue Projekte	• Anwenden einer Audit Map.
Konfiguration der Audit-Map, die für bestehende Projekte verwenden werden soll	• Erstellen einer Audit Map. • Ändern einer Audit Map. • Kopieren einer Audit Map aus einem anderen Projekt.
Anwendung der Audit-Map auf bestehende Projekte	• Anwenden einer Audit Map.

Installierte Audit-Maps

Die Software umfasst mehrere Audit-Maps. Zum Anzeigen oder Ändern einer installierten Audit-Map siehe Abschnitt: Ändern einer Audit Map.

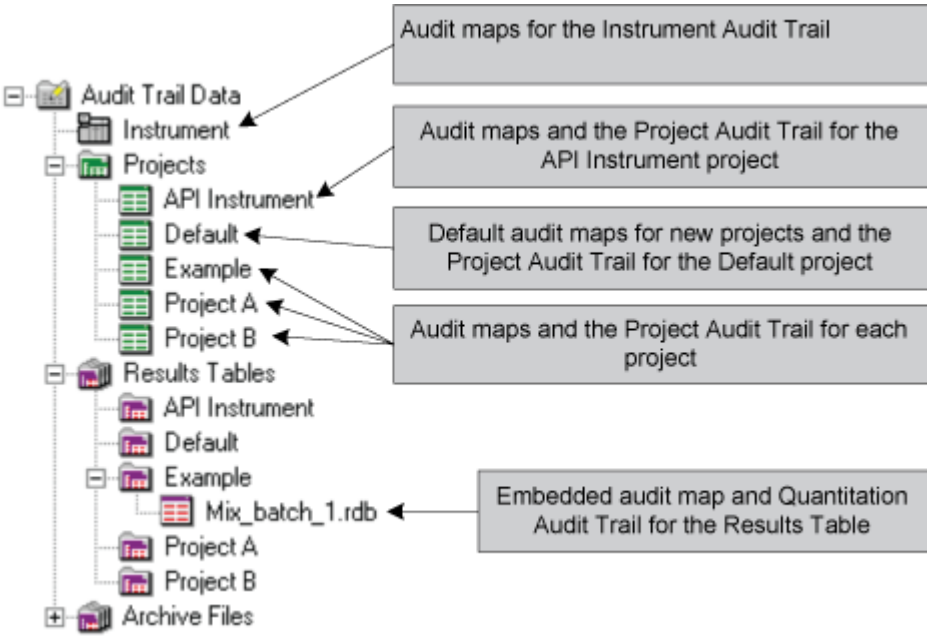
Tabelle 7-3: Installierte Audit-Maps

Audit-Map	Beschreibung
Default Audit Map	Bei der Installation ist die Standard-Audit-Map die aktive Audit-Map für neue Projekte. Standardmäßig werden alle Ereignisse im Hintergrund der Analyst MD-Software überwacht. Wenn die Audit-Trail-Einstellung eines Projekts, das mit einer früheren Version der Analyst MD-Software erstellt wurde, konvertiert wurden, dann enthält die Standard-Audit-Map diese Audit-Konfiguration.
Full Audit Map	Alle Ereignisse werden geprüft. Für alle Ereignisse sind elektronische Signaturen und Gründe erforderlich.
No Audit Map	Es werden keine Ereignisse überprüft.
Quant Only Audit Map	Es werden nur Quantifizierungsereignisse überprüft. Diese Ereignisse erfordern eine elektronische Signatur und einen Grund.
Silent Audit Map	Alle Ereignisse werden geprüft. Für kein Ereignis 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: Audit-Trail-Aufzeichnungen.

Für Informationen zu den Speicherplätzen der Audit-Maps und Audit-Trails im „Audit Trail Manager“ siehe die Abbildung: Abbildung 7-1.

Abbildung 7-1: Audit Trail Manager: Speicherplatz der Audit-Maps und Audit-Trails



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

Arbeiten mit Audit-Maps

Die Analyst MD-Software umfasst mehrere installierte Audit-Maps. Lassen Sie diese anzeigen, um zu entscheiden, ob es einfacher ist, eine oder mehrere Audit-Maps zu modifizieren statt eine neue Audit-Map zu erstellen. Für Beschreibungen der Audit-Maps siehe Abschnitt: Installierte Audit-Maps. Für eine Checkliste der empfohlenen Schritte beim Einrichten von Audits siehe Abschnitt: Einrichten von Audit-Maps.

Wenn eine aktive Audit-Map in Analyst MD oder im Datei-Explorer gelöscht wird, dann verwendet ein Projekt, das diese Audit-Map verwendet, stattdessen die standardmäßige Audit-Map (`Default Audit Map.cam`). Die standardmäßige Audit-Map kann nicht gelöscht werden.

Erstellen einer Audit Map

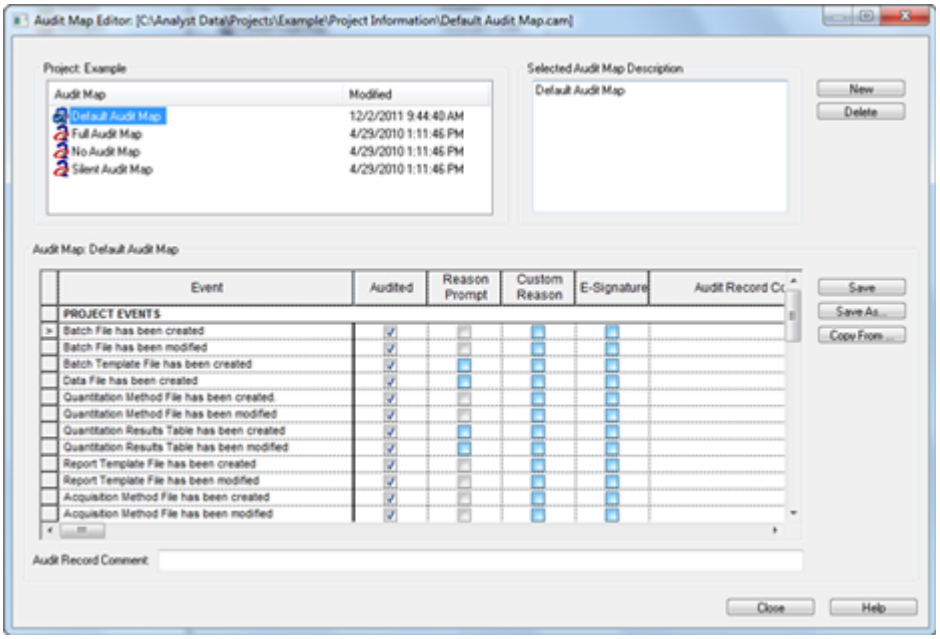
Die aktive Audit Map für ein Projekt bestimmt, welche Ereignisse im Project Audit Trail und in den Quantitation Audit Trails für jede erstellte Ergebnistabelle aufgezeichnet werden.

1. Klicken Sie auf **View** > **Audit Trail Manager**.
   Das Fenster „Audit Trail Manager“ wird geöffnet.
2. Erweitern Sie im linken Fensterbereich den Ordner **Audit Trail Data**.
3. Vergrößern Sie den Ordner **Projects**.
4. Klicken Sie im Abschnitt „Projects“ auf das Projekt, für das eine Audit Map erstellt wird. Um eine Audit Map zur Verwendung mit dem Instrument-Audit-Trail zu erstellen, klicken Sie auf den Ordner `API Instrument`.

Tipp! Um eine Audit Map zur Verwendung mit dem Instrument-Audit-Trail zu erstellen, klicken Sie auf **Instrument** über dem Ordner `Projects`.

5. Klicken Sie auf der Registerkarte **Settings** auf **Edit**.
   Das Dialogfeld „Audit Map Editor“ öffnet sich und die aktive Audit-Map wird angezeigt.

Abbildung 7-2: Dialogfeld „Audit Map Editor“



6. Klicken Sie auf **New**.
   Es wird eine neue Audit Map ohne geprüfte Ereignisse angezeigt.
7. Geben Sie in das Feld **Selected Audit Map Description** gegebenenfalls eine Beschreibung für die Audit Map ein.
8. Konfigurieren Sie jedes Ereignis in der Tabelle **Audit Map** wie folgt:
   - Um das Ereignis zu prüfen, aktivieren Sie das Kontrollkästchen in der Spalte **Audited**.

     Tipp! Um aufeinander folgende Zellen in einer Spalte mit dem gleichen Text zu füllen oder den gleichen Kontrollkästchen-Wert zuzuweisen, geben Sie den Text in der ersten Zeile ein und markieren dann die Zeilen in der Spalte, beginnend mit der ersten Zeile. Klicken Sie mit der rechten Maustaste auf die markierten Zeilen und klicken dann auf **Fill Down**.

   - Wenn Benutzer einen vordefinierten Grund für eine Änderung angeben sollen, wenn das Ereignis eintritt, aktivieren Sie das Kontrollkästchen in der Spalte **Reason Prompt** und geben Sie dann in der Spalte **Predefined Reason** bis zu zehn Gründe ein.

- Wenn Benutzer einen benutzerdefinierten Grund eingeben sollen, aktivieren Sie das Kontrollkästchen in der Spalte **Reason Prompt** und aktivieren dann das Kontrollkästchen in der Spalte **Custom Reason**.
- Um elektronische Signaturen für das Ereignis zu fordern, aktivieren Sie das Kontrollkästchen in der Spalte **E-Signature**.
- Um eine Notiz zur Audit-Konfiguration für dieses Ereignis hinzuzufügen, geben Sie einen Kommentar in die Spalte **Audit Record Comment** ein.

9. Um die „Audit Map“-Konfiguration zu speichern, klicken Sie auf **Save**.

Hinweis: Speichern Sie die Audit Map (mit einer .cam-Erweiterung) im Unterordner **Project Information** des Projektordners, in dem diese verwendet werden soll.

Die Audit Map kann jetzt mit dem Projekt verwendet werden oder in ein anderes Projekt kopiert werden. Siehe die Abschnitte: Anwenden einer Audit Map) oder Kopieren einer Audit Map aus einem anderen Projekt).

Ändern einer Audit Map

Änderungen werden nur auf die Audit Map im ausgewählten Projekt angewendet. In „Results Tables“ eingebettete Audit-Konfigurationen können nicht geändert werden.

VORSICHT: Möglicher Datenverlust. Sie dürfen eine Audit-Map, die von einem anderen Benutzer verändert wird, nicht ebenfalls verändern. Nur die zuletzt vorgenommenen und in der Audit-Map gespeicherten Änderungen bleiben erhalten.

1. Klicken Sie auf **View** > **Audit Trail Manager**.
   Das Fenster „Audit Trail Manager“ wird geöffnet.
2. Erweitern Sie im linken Fensterbereich den Ordner **Audit Trail Data**.
3. Vergrößern Sie den Ordner **Projects**.
4. Klicken Sie im Abschnitt **Projects** auf das Projekt, das die zu ändernde Audit Map enthält.
5. Klicken Sie auf der Registerkarte **Settings** auf **Edit**.
   Das Dialogfeld „Audit Map Editor“ öffnet sich und die aktive Audit-Map wird angezeigt.
6. Im Abschnitt **Projects** klicken Sie auf die Audit Map, die geändert werden soll.
7. In der Audit Map-Tabelle nehmen Sie jegliche Konfigurationsänderungen vor. Für weitere Informationen über die Tabelle klicken Sie auf **Help**.
8. Zum Speichern der Audit Map klicken Sie auf **Save**.

Kopieren einer Audit Map aus einem anderen Projekt

Audit Maps können von einem Projekt in ein anderes kopiert werden.

VORSICHT: Potenziell falsches Ergebnis. Kopieren Sie keine cam-Dateien („Audit Maps“) zwischen den Projekten außerhalb der Analyst MD Software, da dies zu ungenauen Audit-Trails führen kann.

1. Klicken Sie auf **View** > **Audit Trail Manager**.
   Das Fenster „Audit Trail Manager“ wird geöffnet.
2. Erweitern Sie im linken Fensterbereich den Ordner **Audit Trail Data**.
3. Vergrößern Sie den Ordner **Projects**.
4. Klicken Sie im Abschnitt **Projects** auf das Projekt, in das die Audit Map eingefügt werden soll.
5. Klicken Sie auf der Registerkarte **Settings** auf **Edit**.
   Das Dialogfeld „Audit Map Editor“ öffnet sich und die aktive Audit-Map wird angezeigt.
6. Klicken Sie auf **New**.
   Das Dialogfeld „Audit Map Editor“ zeigt eine neue Audit Map ohne geprüfte Ergebnisse.
7. Klicken Sie auf **Copy From**.
   Das Dialogfeld „Open“ wird angezeigt.
8. Navigieren Sie zu und wählen die Audit Map-Datei, die Sie kopieren wollen, und klicken dann auf **Open**. Die Dateien der Audit Map haben die Endung cam und werden im Ordner „Project Information“ für jedes Projekt gespeichert.
   Die ausgewählte Audit Map-Konfiguration wird geöffnet.
9. Klicken Sie zum Speichern der kopierten Audit Map im aktuellen Projekt auf **Save**.

Anwenden einer Audit Map

Wenn eine Audit Map auf einen Instrument Audit Trail oder einen Project Audit Trail angewendet wird, wird sie zur aktiven Audit Map. Die Audit-Konfiguration in der aktiven Audit-Map bestimmt, welche Ereignisse in den Audit-Trails aufgezeichnet werden.

Die aktive Audit Map in einem Projekt enthält die Audit-Konfigurationen für den Project Audit Trail und die Audit-Konfiguration für den Quantitation Audit Trail aller Ergebnistabellen, die erstellt werden.

1. Klicken Sie auf **View** > **Audit Trail Manager**.
   Das Fenster „Audit Trail Manager“ wird geöffnet.
2. Im linken Fensterbereich erweitern Sie den **Audit Trail Data**-Ordner und führen Sie einen der folgenden Schritte aus:
   - Um eine Audit Map auf den **Instrument Audit Trail** anzuwenden, klicken Sie auf **Instrument**.
   - Um eine Audit Map auf ein Projekt anzuwenden, erweitern Sie den Ordner **Projects** und klicken Sie dann auf das Projekt, auf das die Audit Map angewendet werden soll.
   - Um die standardmäßig aktive Audit Map für neue Projekte festzulegen, erweitern Sie den Ordner **Projects** und klicken Sie dann auf **Default**.
3. Klicken Sie im rechten Fensterbereich auf die Registerkarte **Settings**.
4. Im Feld **Available Audit Trail Maps** klicken Sie auf die Audit Map, die angewendet werden soll.
5. Klicken Sie auf **Apply**.

Anzeigen, Drucken und Durchsuchen von Audit Trails

Dieser Abschnitt enthält Informationen zum Anzeigen von Audit Trails, archivierten Audit Trails und Einträgen des Instrumentenwartungsprotokolls. Er enthält auch Anweisungen zum Drucken, Suchen und Sortieren von Audit-Aufzeichnungen innerhalb von Audit Trails.

Anzeigen eines Audit-Trails

1. Klicken Sie auf **View** > **Audit Trail Manager**.
   Das Fenster „Audit Trail Manager“ wird geöffnet.
2. Im linken Fensterbereich erweitern Sie den **Audit Trail Data** -Ordner und führen Sie einen der folgenden Schritte aus:
   - Wenn Sie einen Audit Trail anzeigen wollen, klicken Sie auf **Instrument**. Um gerätespezifische Ereignisse anzeigen zu lassen, wie z.B. Massenkalibrierungstabelle(n), lassen Sie den Instrument Audit Trail auf dem Computer anzeigen, der direkt an das Massenspektrometer angeschlossen ist.
   - Um einen Project Audit Trail anzuzeigen, erweitern Sie den Ordner **Projects** und klicken Sie dann auf das Projekt, das den Audit Trail enthält.
   - Um einen Quantitation Audit Trail anzuzeigen, erweitern Sie den Ordner **Results Tables** , erweitern den entsprechenden Projektordner und klicken dann auf die **Results Table**-Datei für diesen Audit Trail.

   Tipp!

   - Wenn sich ein geprüftes Ereignis auf eine wiff-Datei bezieht, dann öffnen Sie die wiff-Datei aus dem **Audit Trail**. Klicken Sie in der Spalte **Change Description** auf den Link zur Datei.
   - Zum Anzeigen der Proben-Peak-Daten unter Verwendung einer Quantifizierungsmethode und eines Probenindex, die in einer Audit-Aufzeichnung gespeichert sind, öffnen Sie die entsprechende **Results Table** und klicken Sie dann in der Spalte **History** des Audit-Trails auf **Review**. Wenn die Quantifizierungsmethode, die während der Erstellung der Audit-Aufzeichnung verwendet wurde, geändert wurde, dann werden für den Peak möglicherweise andere Ergebnisse als die ursprünglichen Ergebnisse angezeigt. Um die ursprünglichen Ergebnisse anzuzeigen, verwenden Sie die entsprechende Version der Software.

In eine „Results Table“ eingebettete Audit-Konfiguration anzeigen

Die Audit-Konfiguration, die für eine „Results Table“ verwendet wird, wird in die „Results Table“-Datei eingebettet, wenn die „Results Table“ erstellt wird. Die Ergebnistabellen-Audit-Konfiguration kann nicht geändert werden. Der neben dem Audit-Map-Namen angezeigte Zeitstempel gibt an, wann die Audit Map zuletzt gespeichert wurde, die zur Einbindung der Konfiguration verwendet wurde.

1. Klicken Sie auf **View** > **Audit Trail Manager.**
   Das Fenster „Audit Trail Manager“ wird geöffnet.
2. Erweitern Sie im linken Fensterbereich den Ordner **Audit Trail Data**.
3. Vergrößern Sie den Ordner **Results Tables**.
4. Im Abschnitt **Results Tables** erweitern Sie das Projekt, das die „Results Table“ enthält, für das Sie die Audit Map anzeigen lassen wollen.
5. Klicken Sie die **Results Table**-Datei, für die Sie die Audit Map anzeigen lassen wollen.
   Der Audit Trail wird im rechten Fensterbereich angezeigt.
6. Klicken Sie auf der Registerkarte „Settings“ auf **Details**.

   Das Dialogfeld „Results Table Audit Trail Settings“ öffnet sich und zeigt die Konfiguration des Prüfpfades für die „Results Table“ an.

Anzeigen von Details einer Audit-Aufzeichnung im Instrument Audit Trail

Der Benutzer kann Details der folgenden geprüften Ereignisse ansehen: Änderungen in der Massenkalibriertabelle, Änderungen in der Auflösungstabelle oder Einträge im Instrument-Wartungsprotokoll.

1. Klicken Sie auf **View** > **Audit Trail Manager**.
   Das Fenster „Audit Trail Manager“ wird geöffnet.
2. Erweitern Sie im linken Fensterbereich den Ordner **Audit Trail Data**.
3. Klicken Sie im Abschnitt **Audit Trail Data** auf **Instrument**. Wenn der Audit Trail nicht angezeigt wird, klicken Sie im rechten Fensterbereich auf die Registerkarte **History**.
   Der Audit-Trail wird geöffnet.
4. Für jeden Datensatz mit zusätzlichen Details klicken Sie auf **Review** in der Spalte **History**.

Anzeigen eines archivierten Audit-Trails

Nachdem ein Instrument Audit Trail oder ein Projekt Audit Trail 1000 Audit-Aufzeichnungen enthält, archiviert die Analyst MD Software diese Aufzeichnungen automatisch und beginnt einen neuen Audit Trail. Die Audit Trail-Dateien werden mit einem Namen archiviert, der den Typ des Audit Trails und das Datum und die Uhrzeit angibt, z. B. PAT-Archive-201609300820.ata.

1. Klicken Sie auf **View** > **Audit Trail Manager**.
   Das Fenster „Audit Trail Manager“ wird geöffnet.
2. Erweitern Sie im linken Fensterbereich den Ordner **Audit Trail Data**.
3. Vergrößern Sie den Ordner **Archive Files**.
4. Erweitern Sie im Abschnitt **Archive Files** das Projekt, das den archivierten Audit-Trail, der angezeigt werden soll.
5. Klicken Sie auf den Audit Trail, den Sie anzeigen möchten.

Der archivierte Audit Trail wird im rechten Fensterbereich angezeigt.

6. Wenn der Audit Trail nicht geöffnet wird, klicken Sie im rechten Fensterbereich auf die Registerkarte **History**.
   Der Audit-Trail wird geöffnet.

Tipp! Alternativ können einen archivierten Audit Trail durch Klicken mit der rechten Maustaste im linken Fensterbereich und einem Klick auf **Open Archives** öffnen. Das Dialogfeld „Open“ wird angezeigt. Navigieren Sie zum entsprechenden Projektordner und wählen Sie dann aus dem Ordner **Project Information** die archivierte Audit Trail-Datei. Diese Dateien haben die Endung .ata.

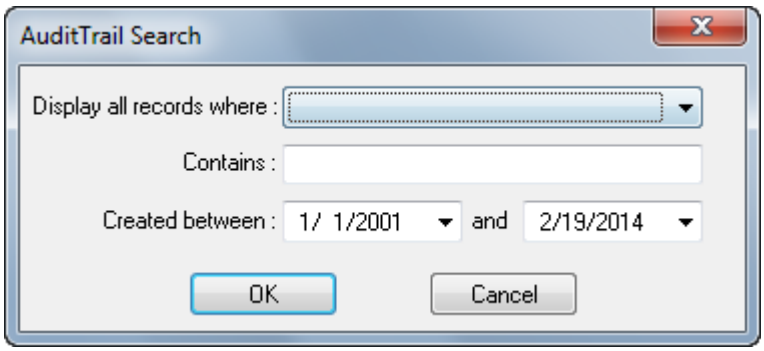
Drucken eines Audit-Trails

1. Klicken Sie auf **View** > **Audit Trail Manager**.
   Das Fenster „Audit Trail Manager“ wird geöffnet.
2. Wählen Sie den Audit Trail aus.
3. Auf der Registerkarte **History** klicken Sie auf **Print** und führen einen der folgenden Schritte aus:
   - Um die aktuelle Seite zu drucken, klicken Sie auf **Current Page**.
   - Um alle Seiten im Audit Trail zu drucken, klicken Sie auf **All Pages**.

Suchen nach einer Audit-Aufzeichnung

1. Klicken Sie auf **View** > **Audit Trail Manager**.
   Das Fenster „Audit Trail Manager“ wird geöffnet.
2. Wählen Sie den Audit Trail aus.
3. Zeigen Sie den Audit Trail an, den Sie durchsuchen möchten.
4. Klicken Sie mit der rechten Maustaste in die Registerkarte **History** und klicken dann auf **Search**.

Abbildung 7-3: Dialogfeld „Audit Trail Search“



5. Verwenden Sie die Liste **Display all records where** und das Feld **Contains**, um die Datensätze zu wählen, die gefunden werden sollen.

6. Falls erforderlich wählen Sie das Start- und Enddatum aus den Listen **Created between**.
7. Klicken Sie auf **OK**.
   Nur Datensätze, die die Kriterien erfüllen, werden aufgelistet.

Tipp! Um alle Datensätze aufzulisten, klicken Sie auf **All**. Um die Datensätze numerisch, alphabetisch oder nach Datum zu sortieren, klicken Sie auf die entsprechende Spaltenüberschrift.

Audit-Trails A

In diesem Abschnitt finden Sie Listen aller geprüften Ereignisse, die in den Geräte-, Projekt- und Quantifizierungs-Audit-Trails gespeichert sind.

Für jede geprüfte Änderung einer Datei oder jedes geprüfte Ereignis werden die folgenden Informationen gespeichert:

- Datensatz-Nummer
- Datum und Zeitstempel
- Benutzername
- Vollständiger Benutzername
- Analyst MD Software-Modul
- Beschreibung der Änderung
- Grund für die Änderung, wenn erforderlich
- Elektronische Signatur, wenn erforderlich

Audit-Trail-Aufzeichnungen

Bei den Geräte-, Projekt- und Quantifizierungs-Audit-Trails handelt es sich um verschlüsselte Dateien. Alle anderen Audit-Trail-Dateien werden in den Projektverzeichnissen unter dem Stammverzeichnis gespeichert.

Für jede geprüfte Änderung einer Datei oder jedes geprüfte Ereignis werden die folgenden Informationen gespeichert:

- Datensatz-Nummer
- Datum und Zeitstempel
- Benutzername
- Vollständiger Benutzername
- Analyst MD-Software-Modul
- Beschreibung der Änderung
- Grund für die Änderung, wenn erforderlich
- Elektronische Signatur, wenn erforderlich

Audit-Trail-Archive

Audit-Aufzeichnungen sammeln sich im Projekt-Audit-Trail und im Geräte-Audit-Trail an. Die resultierenden Dateien können sehr groß werden und daher schwierig zu navigieren und zu verwalten sein. Quantifizierungs-Audit-Trails haben in der Regel eine kleinere, überschaubarere Anzahl von Datensätzen.

Wenn ein Geräte-Audit-Trail oder ein Projekt-Audit-Trail 1000 Aufzeichnungen erreicht hat, wird eine letzte Aufzeichnung hinzugefügt, die besagt, dass die Datei archiviert wurde. Der Audit-Trail wird automatisch im Ordner „Project Information“ mit einem Namen gespeichert, der den Typ des Audit-Trails sowie das Datum und die Uhrzeit angibt, z. B. „`PAT-Archive-201609300820.ata`“. Es wird ein neuer Geräte-Audit-Trail oder Projekt-Audit-Trail erstellt und die erste Aufzeichnung des archivierten Audit-Trails gibt den Pfad an.

Ereignisse im Geräte-Audit-Trail

Jeder Computer verfügt über einen Geräte-Audit-Trail. In diesem Audit-Trail werden Ereignisse, wie beispielsweise Ergänzungen oder der Austausch von Massenkalibrierungstabellen oder Auflösungstabellen, Änderungen der Systemkonfiguration, sicherheitsrelevante Ereignisse und Einträge im Geräte-Wartungsprotokoll, aufgezeichnet. Für Computer, die nicht direkt an ein Massenspektrometer angeschlossen sind, zeichnet der Geräte-Audit-Trail nur sicherheitsrelevante Ereignisse auf.

Der Geräte-Audit-Trail protokolliert die folgenden Ereignisse:

- Massenkalibrierungstabellen wurden ersetzt
- Massenkalibrierungstabellen wurden hinzugefügt
- Auflösungstabellen wurden ersetzt
- Auflösungstabellen wurden hinzugefügt
- Hardwareprofil wurde aktiviert[4]
- Hardwareprofil wurde deaktiviert[4]
- Es wurde ein Eintrag im Geräte-Wartungsprotokoll vorgenommen
- Chargendatei wurde übergeben[4]
- Probe wurde zur Erfassung übergeben[4]
- Probe wurde in der Chargendatei von Position x zu Position y verschoben[4]
- Charge verschieben[4]
- Probe(n) neu erfassen[4]
- Massenkalibrierungstabellen und Auflösungstabellen haben sich geändert
- Auflösungstabelle(n) wurden ersetzt - Keine Eingabeaufforderung[4]
- Geräteeinstellungen wurden geändert
- Gerätekalibrierungsgenehmigung
- Massenkalibrierungstabelle(n) wurden ersetzt[4]
- Benutzer hat sich angemeldet[4]
- Benutzer hat sich abgemeldet[4]
- Benutzeranmeldung ist fehlgeschlagen[4]

[4] Dieses Ereignis kann aus gutem Grund nicht geprüft werden. Es kann im Hintergrund geprüft oder nicht geprüft werden.

- Sicherheitsmitteilung versendet[4]
- Die Sicherheitskonfiguration wurde geändert[4]
- Duo-Ventilschalter-Zähler wurde zurückgesetzt
- Benutzer wurde hinzugefügt[4]
- Benutzer wurde gelöscht[4]
- Benutzertyp wurde hinzugefügt[4]
- Benutzertyp wurde gelöscht[4]
- Benutzertyp wurde geändert[4]
- Benutzermodus wurde geändert[4]
- Benutzer hat Benutzertyp geändert[4]
- Erfassungskonto wurde geändert[4]
- Bildschirmsperre wurde geändert[4]
- Das automatische Abmelden wurde geändert[4]
- Gerät wurde hinzugefügt[4]
- Gerät wurde gelöscht[4]
- Rolle im Projekt hinzugefügt[4]
- Rolle im Projekt geändert[4]
- Rolle im Projekt gelöscht[4]
- Sicherheit im Projekt geändert[4]
- Tune-Parameter-Einstellungen geändert[4]

Ereignisse des Projekt-Audit-Trails

Jedes Projekt hat einen Projekt-Audit-Trail. In diesem Audit-Trail werden Ereignisse aufgezeichnet, wie z. B. die Erstellung, Änderung und Löschung von Projekt-, Daten-, Quantifizierungs-, Methoden-, Chargen-, Tuning-, „Results Table“- und Berichtsvorlagendateien, das Öffnen und Schließen von Modulen sowie Druckereignisse.

Der Projekt-Audit-Trail kann die folgenden Ereignisse protokollieren:

- Audit-Map wurde erstellt[5]
- Audit-Map wurde geändert[5]
- Audit-Map wurde gelöscht[5]
- Chargendatei wurde erstellt[6]
- Chargendatei wurde geändert[6]

[5] Dieses Ereignis wird immer im Hintergrund geprüft und erscheint nicht im Dialogfeld „Audit Map Editor“.
[6] Dieses Ereignis kann aus gutem Grund nicht geprüft werden. Es kann im Hintergrund geprüft oder nicht geprüft werden.

- Chargenvorlagendatei wurde erstellt[6]
- Datendatei wurde erstellt[6]
- Quantifizierungsmethodendatei wurde erstellt[6]
- Quantifizierungsmethodendatei wurde geändert[6]
- Quantifizierungs-„Results Table“ wurde erstellt[6]
- Quantifizierungs-„Results Table“ wurde geändert[6]
- Berichtsvorlagendatei wurde erstellt
- Berichtsvorlagendatei wurde geändert
- Erfassungsmethodendatei wurde erstellt.
- Erfassungsmethodendatei wurde geändert.
- Geöffnetes Modul[6]
- Geschlossenes Modul[6]
- Probe wurde zur Datendatei hinzugefügt[6]
- Dokument wird auf Drucker gedruckt
- Druckvorgang für Dokument auf Drucker beendet[6]
- Datendatei wurde geöffnet[6]
- „Explore History“-Datei wurde gespeichert
- Verarbeitete Daten-Datei wurde gespeichert.
- Prüfsummendatei[6]
- Projekteinstellungen wurden geändert[7]
- Der Verarbeitungsalgorithmus wurde geändert[6]

Ereignisse des Quantitation Audit Trail

Ein Quantitation Audit Trail wird immer in der Datei der Ergebnistabellen gespeichert. Wenn eine „Results Table“ erstellt wird, wird die im Projekt aktive Audit Map in der „Results Table“-Datei zur Verwendung mit dem Quantifizierungs-Prüfpfad gespeichert. Diese eingebettete Audit Map kann nach der Erstellung der „Results Table“ nicht mehr geändert werden. Alle Änderungen an der Ergebnistabelle werden anhand der eingebetteten Audit Map geprüft. Änderungen an der (im Projekt) aktiven Audit Map werden in den bestehenden Ergebnistabellen nicht aktualisiert, aber alle neuen Ergebnistabellen verwenden die geänderte aktive Audit Map.

Eine „Quantitation Audit Trail“-Ereignisbeschreibung umfasst die an den Daten durchgeführte Operation wie z.B. aus einer Kalibrierung entfernte Punkte, automatische und manuelle Basislinien-Anpassungen und Änderungen an Kurvenanpassungen.

[7] Dieses Ereignis wird immer geprüft.

In einem Quantitation Audit Trail enthalten Audit-Aufzeichnungen enthalten weitere Details, die im Zusammenhang mit der Integration von Probenpeaks stehen. Diese Aufzeichnungen umfassen die letzten Quantifizierungsprozessparameter, die mit jeder Probe in der Ergebnistabelle verknüpft sind. Zum Beispiel könnte der Audit Trail für eine Ergebnistabelle die Parameter enthalten, die für alle manuellen Korrekturen an den automatischen Peak-Integrationen verwendet wurden.

Der Quantitation Audit Trail kann die folgenden Ereignisse protokollieren:

- Quantifizierungsmethode wurde aktualisiert
- Quantifizierungspeak wurde wieder auf den ursprünglichen Peak zurückgesetzt
- Quantifizierungspeak wurde integriert
- Ergebnistabelle wurde erstellt
- Quantifizierungsmethode wurde geändert
- Dateien wurden zur Ergebnistabelle hinzugefügt
- Dateien wurden aus der Ergebnistabelle entfernt
- Ergebnistabelle wurde vom QA Reviewer (Qualitätssicherungsprüfer) aufgerufen
- Ergebnistabelle wurde gespeichert
- Ergebnistabellen-Audit-Trail-Einträge wurden entfernt.
- „Use IT“ wurde geändert
- „Sample Name“ wurde geändert
- „Sample ID“ wurde geändert
- „Sample Type“ wurde geändert
- „Sample Comment“ wurde geändert
- „Sample Annotation“ wurde geändert
- „Weight to Volume Ratio“ wurde geändert
- „Dilution Factor“ wurde geändert
- „Concentration“ wurde geändert
- „Analyt Annotation“ wurde geändert
- Formelspalte wurde hinzugefügt
- Formelname wurde geändert
- Formel-String wurde verändert
- Formelspalte wurde entfernt
- „Custom Title“ wurde geändert
- Proben wurden hinzugefügt/entfernt

AAC Audit-Trail

Jeder Analyst Administrator Console (AAC) Server verfügt über einen entsprechenden Audit-Trail. Diese Funktion wird nicht unterstützt von der Analyst MD Software.

Zusätzliche Sicherheitsanpassungen B

Dieser Abschnitt enthält Informationen zu zusätzlichen Funktionen, die die Analyst MD Software zur Sicherung von Daten anbietet.

Dateiänderungen („Explore Processing“)

Die Datei „Explore Processing History“ enthält eine Aufzeichnung der Änderungen von Verarbeitungsparametern, die bezüglich einer Datendatei vorgenommenen wurden. Diese Aufzeichnungen müssen manuell erstellt werden, um eine Aufzeichnung über die vorgenommenen Änderungen zu haben. Nur die aktuellen Änderungen werden gespeichert. Nachdem eine „Explore Processing History“-Datei erstellt wurde, kann diese in der Analyst MD Software nicht geändert oder gelöscht werden.

Nachdem das Protokoll der Änderungen in einer Datendatei gespeichert wurde, verwenden Sie dieses Protokoll, um die Datei an einem beliebigen Zeitpunkt bei Änderungen einzusehen. Benutzer können dieses Protokoll nicht ändern oder eine frühere Version der Datei über das Protokoll speichern.

Die „Explore Processing History“-Dateien zeichnen folgende Prozessparameter auf:

- „Smooth/Previous Point Weight“
- „Smooth/Current Point Weight“
- „Smooth/Next Point Weight“
- „Gaussian Smooth/Filter Width“
- „Gaussian Smooth/Distance“
- „Centroid Options/Merge Distance“
- „Centroid Options/Minimum Width“
- „Centroid Options/Use Peak Maximum for X Value“
- „Baseline Subtract/Windows Width“
- „Threshold“
- „Noise Filter/Minimum Peak Width“
- „Base Peak Chromatogram/Mass Tolerance“
- „Add“
- „Subtract“

Erstellen von „Explore Processing History“-Dateien

Eine „Explore Processing History“-Datei (.eph) kann innerhalb der Analyst MD Software nicht geändert oder gelöscht werden.

Klicken Sie im Modus **Explore** mit der rechten Maustaste in das Fenster einer Datendatei und anschließend auf **Save Explore History**. „Explore Processing History“-Dateien werden im Unterordner „Processing Methods“ des Projekts gespeichert.

Tipp! Um den Überblick über „Explore Processing History“-Dateien zu behalten, speichern Sie die Protokolldatei mit einem der Datendatei ähnlichen Namen.

Eine „Explore Processing History“-Datei anzeigen

1. Klicken Sie auf **File** > **Open**.
   Das Dialogfeld „Open“ wird angezeigt.
2. Klicken Sie in der Liste **Files of type** auf **Explore History Files (eph)**.
3. Im Feld **Files** klicken Sie auf die Datei und anschließend auf **OK**.
   Die wiff-Datei wird in der Datei „Explore Processing History“ in einem Fenster darunter geöffnet.
4. Klicken Sie zum Anzeigen der wiff-Datei mit Verarbeitungsparametern auf die Registerkarte **Review** unter der Spalte „History“.
5. Klicken Sie zum Drucken des Fensters „Explore Processing“ mit der rechten Maustaste auf die Registerkarte **History**, dann auf **Print** und dann entweder auf **Current Page** oder auf **All Pages**.
6. Zur Anzeige des aktuellen Datenverarbeitungs-Protokolls der einer Datendatei im aktiven Teilfenster klicken Sie im **Explore**-Modus auf **Explore** > **Show** > **Show History.** Das angezeigte Protokoll wird nicht automatisch gespeichert und kann zur Prüfung der Verarbeitung nicht verwendet werden.

Hinzufügen eines Eintrags in das Instrument-Wartungsprotokoll

Wenn das Massenspektrometer gewartet wird, wie z.B. Systemwartungen, Reinigung und Überprüfung der Referenzen, notieren Sie die Wartungsdetails im Instrument Audit Trail über das Instrument-Wartungsprotokoll.

1. Klicken Sie auf **View** > **Audit Trail Manager**.
   Das Fenster „Audit Trail Manager“ wird geöffnet.
2. Erweitern Sie im linken Fensterbereich den Ordner **Audit Trail Data**.
3. Im Abschnitt „Audit Trail Data“ klicken Sie auf **Instrument**.
4. Öffnen Sie im rechten Fensterbereich die Registerkarte „Maintenance Log“.
5. Geben Sie die Wartungsinformationen in die entsprechenden Felder ein.
6. Klicken Sie zum Speichern des Protokolleintrags auf **Submit**.

Einen Eintrag des Instrument-Wartungsprotokolls anzeigen

1. Klicken Sie auf **View** > **Audit Trail Manager**.
   Das Fenster „Audit Trail Manager“ wird geöffnet.
2. Erweitern Sie im linken Fensterbereich den Ordner **Audit Trail Data**.
3. Im Abschnitt „Audit Trail Data“ klicken Sie auf **Instrument**.
4. Wenn der Audit-Trail nicht angezeigt wird, dann öffnen Sie im rechten Fensterbereich die Registerkarte „History“.
   Der Audit-Trail wird geöffnet.
5. Um einen bestimmten Eintrag im Instrument-Wartungsprotokoll anzuzeigen, klicken Sie auf **Review** in der Spalte **History**.
   Das Dialogfeld „Audit Trail History“ wird geöffnet und zeigt die Details zum Eintrag im „Log“ an.

   Tipp! Um alle „Log“-Einträge im Instrument Audit Trail zu finden, klicken Sie auf **Search**. Im Dialogfeld „Audit Trail Search“ verwenden Sie die Optionen, um alle Datensätze anzuzeigen, in denen die „Change Description“ eine „Instrument Maintenance“ enthält.

Konfigurieren der E-Mail-Benachrichtigung

Die Analyst MD Software kann so konfiguriert werden, dass eine E-Mail-Benachrichtigung nach drei Anmeldefehlern innerhalb eines Tages gesendet wird. Diese E-Mail-Benachrichtigung ist nur dann verfügbar, wenn die Software im „Integrated“ oder „Mixed Mode“ arbeitet. Informationen über Sicherheitsmodi finden Sie im Abschnitt: Analyst MD-Software und Windows-Sicherheit: Zusammenarbeit.

Der Empfänger der E-Mail muss Zugang zu einem gültigen Account (Konto) auf einem SMTP-kompatiblen E-Mail-Server haben und der Computer mit der Analyst MD Software muss Zugriff auf einen SMTP-Server haben.

1. Klicken Sie auf **View** > **Audit Trail Manager**.
   Das Fenster „Audit Trail Manager“ wird geöffnet.
2. Klicken Sie mit der rechten Maustaste im linken Fensterbereich des Audit Trail Manager auf **Options** und dann auf **E-Mail Notification Settings**.
   Das Dialogfeld „Audit Trail Options“ wird geöffnet und zeigt die Registerkarte **Security Mail Settings** an.
3. Aktivieren Sie das Kontrollkästchen **Send e-mail message(s) after 3 logon failures within 24hr.**.
4. Im Feld **SMTP Server** geben Sie den Namen des SMTP-Servers ein.

   Hinweis: Das SMTP-Konto sendet Mails an den E-Mail-Server. Verwenden Sie Ihre E-Mail-Anwendung, um den SMTP-Server festzulegen.

5. Geben Sie im Feld **Port Number** die Port-Nummer ein.
   Die Schaltfläche **Default** fügt die Standard-Port-Nummer „25“ ein.

6. Geben Sie im Feld **To** die E-Mail-Adresse ein, an die die Nachricht gesendet werden soll. Beispiel: username@domain.com.
7. Geben Sie im Feld **From** den Namen ein, der im Feld **From** der Nachricht angezeigt werden soll. Geben Sie z.B. den Namen des Computers ein, um aufzuzeichnen, auf welchem Computer die Anmeldefehler auftraten. Der Wert im Feld **From** darf keine Leerzeichen enthalten.
8. Im Feld **Subject** geben Sie den Betreff der Nachricht ein.
9. Im Feld **Message** geben Sie den Text der Nachricht ein.
10. Um die Konfiguration zu überprüfen, klicken Sie auf **Send Test Mail**.
11. Um die Konfiguration zu speichern, klicken Sie auf **OK**.

Hinweis: Wenn die E-Mail-Benachrichtigung nicht in der **Inbox** zu finden ist, überprüfen Sie den Ordner **Junk E-mail**.

Tipp! Um die E-Mail-Benachrichtigung zu deaktivieren, deaktivieren Sie das Kontrollkästchen **Send email message(s) after 3 logon failures within 24hr.**.

Datendatei-Prüfsumme

Wir empfehlen den Nutzern, Datendatei-Prüfsummen zu verwenden. Die Prüfsummenfunktion ist eine zyklische Redundanzprüfung, mit der die Integrität der Datendatei überprüft wird. Die Prüfsummenfunktion wird standardmäßig für die Neuinstallation der Analyst MD Software aktiviert. Wenn Benutzer ein Upgrade auf die aktuelle Version der Analyst MD Software durchführen, bleibt die Prüfsummeneinstellung von vor der Aktualisierung bestehen.

Die Prüfsummenfunktion muss verwendet werden, wenn das Massenspektrometer als IVD-Gerät verwendet 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.

Überprüfen der Datendatei-Prüfsumme

Wenn eine Datendatei geöffnet wird, kann der Benutzer die Prüfsumme überprüfen. Dieser Abschnitt enthält Schritte zur Überprüfung einer Prüfsumme und zum Aktivieren und Deaktivieren der Funktion „Data File Checksum“.

Die Berechnung der Prüfsumme kann bei großen Dateien über eine Minute dauern. Während der Erfassung kann die Prüfsumme der Datei, die gerade erstellt wird, nicht überprüft werden.

1. Klicken Sie auf **File** > **Open Data File**.
   Das Dialogfeld „Select Sample“ wird geöffnet.
2. Wählen Sie im Feld **Data Files** eine Datendatei (wiff) aus.
3. Klicken Sie auf **Verify Checksum**.

   Das Meldungsdialogfeld „ExplorDir“ wird geöffnet und zeigt das Ergebnis des Prüfsummenvergleichs als „Valid“, „Invalid“ oder „Not found“ an.

Aktivieren oder Deaktivieren der Funktion „Data File Checksum“

Die Analyst MD-Software zeigt an, ob die Funktion „Data File Checksum“ aktiviert ist; dies ist an einem Häkchen neben dem Befehl im Kontextmenü des Audit Trail Managers erkennbar.

1. Klicken Sie auf **View** > **Audit Trail Manager**.
   Das Fenster „Audit Trail Manager“ wird geöffnet.
2. Klicken Sie mit der rechten Maustaste in den linken Fensterbereich des Audit Trail Manager und dann auf **Options**.
3. Klicken Sie auf **Data File Checksum**.

   Wenn die Funktion „Data File Checksum“ aktiviert ist, erscheint neben dem Befehl ein Häkchen. Wenn die Funktion „Data File Checksum“ deaktiviert ist, verschwindet das Häkchen.

Besonderes Erfassungskonto C

Hinweis: SCIEX unterstützt die Verwendung der Netzwerkerfassungs-Funktion mit der Analyst MD Software.

In einer regulierten Umgebung, in der Daten in einem Netzwerkordner erfasst werden, verfügen die meisten Benutzer für gewöhnlich nicht über Berechtigungen zum Löschen für den Zielordner. Dies kann zu Problemen führen, da die Analyst MD Software einen Löschzugriff zum erfolgreichen Erfassen von Daten in einen Netzwerkordner erfordert.

Die SAA-Funktion (Special Acquisition Account, besonderes Erfassungskonto) unterstützt die Netzwerkerfassung in einer geschlossenen Netzwerkumgebung, indem Berechtigungen zum Löschen nur an den AnalystService vergeben werden. Um diese Funktion zu aktivieren, erstellt der Laboradministrator ein Konto mit der Berechtigung „Vollzugriff“ für die entsprechenden Ordner und gibt dann dieses Konto in der Gruppe „Special Acquisition Administrator Account“ im Dialogfeld „Security Configuration“ in der Analyst MD Software an. Die Analyst MD Software kann dann erfolgreich Daten erfassen, obwohl die meisten Benutzer über keine Berechtigungen zum Löschen verfügen. Informationen über das Auswählen eines Erfassungskontos finden Sie im Abschnitt: Ein Erfassungskonto auswählen.

Das SAA muss Folgendes aufweisen:

- Berechtigung „Vollzugriff“ (empfohlen) oder „Ändern“ (Minimum) für den Serverdatenordner.
- Berechtigung „Vollzugriff“ (empfohlen) oder „Ändern“ (Minimum) für den Ordner `WIFF_CACHE_BACKUP`.

Folgendes ist für das SAA nicht erforderlich:

- Es muss nicht zur Administratorgruppe auf dem Computer gehören.
- Es muss nicht zum Analyst Administrator Console (AAC) Benutzer-Pool, der Konsolen-Administrator-Arbeitsgruppe oder einer anderen Arbeitsgruppe gehören.
- Es muss nicht in der Sicherheitsdatenbank der Analyst MD Software vorhanden sein.

Kontaktangaben

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.

Für die Anzeige des Dokuments wird der Adobe Acrobat Reader benötigt. Um sich die neueste Version herunterzuladen, besuchen Sie https://get.adobe.com/reader.

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

Informationen zur Hardware-Produktdokumentation finden Sie auf der mit dem System oder der Komponente gelieferten *Customer Reference*-DVD.

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