

Veiledning for laboratorieleder

SCIEX OS-programvare



Dette dokumentet blir levert til kunder som har kjøpt SCIEX-utstyr, og det er beregnet på bruk under betjening av dette SCIEX-utstyret. Dette dokumentet er beskyttet av opphavsrett, og all reproduksjon av dette dokumentet eller deler av dette dokumentet er strengt forbudt, bortsett fra i den grad SCIEX har gitt skriftlig tillatelse.

Programvare som kan beskrives i dette dokumentet leveres under en lisensavtale. Det er i strid med loven å kopiere, modifisere eller distribuere programvaren på noe som helst medium, unntatt som spesifikt tillatt i lisensavtalen. Videre kan lisensavtalen forby demontering, omvendt konstruksjon eller dekompilering av programvaren for alle formål. Garantier gjelder som angitt i lisensavtalen.

Deler av dette dokumentet kan henvise til andre produsenter og/eller deres produkter, som kan inneholde deler hvis navn er registrert som varemerker og/eller fungerer som varemerker for deres respektive eiere. Enhver slik bruk er kun ment for å betegne produsentens produkter, og innebærer ikke noen rett og/eller lisens til å bruke eller tillate andre å bruke disse produsentenes navn og/eller deres produktnavn som varemerker.

SCIEX-garantier er begrenset til de uttrykkelige garantiene som gis på tidspunktet for salg eller lisens av produktene, og de utgjør SCIEX' eneste og eksklusive representasjoner, garantier og forpliktelser. SCIEX gir ingen andre garantier av noe slag, uttrykt eller underforstått, inkludert og uten begrensning, garantier for salgbarhet eller egnethet for et bestemt formål, enten det stammer fra en statutt eller på annen måte fra lovverk eller handlingsforløp eller handelsskikk, som alle fraskrives uttrykkelig, og SCIEX påtar seg intet ansvar eller usikre forpliktelser, inkludert indirekte skader eller følgeskader, for noen former for bruk utført av kjøperen eller for eventuelle ugunstige omstendigheter som oppstår som følge av bruken.

SCIEX klinisk diagnostisk portefølje er for *in vitro* diagnostisk bruk. Produkt(ene) er ikke tilgjengelig i alle land. Kontakt din lokale representant eller se sciex.com/diagnostics for informasjon om tilgjengelighet. Alle andre produkter er kun til forskningsbruk. Ikke til bruk i diagnostiske prosedyrer.

Varemerker og/eller registrerte varemerker som er nevnt her, inkludert tilknyttede logoer, tilhører AB Sciex Pte. Ltd., eller deres respektive eiere i USA og/eller visse andre land (se sciex.com/trademarks).

AB Sciex™ brukes under lisens.

© 2026 DH Tech. Dev. Pte. Ltd.



Innhold

Kapittel 1: Introduksjon	6
Kapittel 2: Oversikt over sikkerhetskongfigurasjon	7
Sikkerhet og overholdelse av forskrifter	7
Sikkerhetskrav	7
SCIEX OS-programvare og Windows-sikkerhet: Samarbeid	7
revisjonsspor i SCIEX OS-programvaren og Windows	8
Veiledning for kundesikkerhet: Sikkerhetskopier	8
21 CFR del 11	9
Systemkongfigurasjon	9
Kongfigurerer Windows-sikkerhet	9
Brukere og grupper	10
Active Directory-støtte	10
Windows-filsystem	11
Fil- og mappetillatelser	11
Systemrevisjoner	11
Hendelseslogger	11
Windows-varsler	12
Kapittel 3: Elektronisk lisensiering	13
Lån en serverbasert elektronisk lisens	13
Returner en serverbasert elektronisk lisens	14
Kapittel 4: tilgangskontroll	16
Plassering av sikkerhetsinformasjon	16
Arbeidsflyt for programvaresikkerhet	16
Installer programvaren SCIEX OS	17
Systemkrav	18
Forhåndsinnstilte revisjonsalternativer	18
Kongfigurer sikkerhetsmodusen	18
Velge sikkerhetsmodus	19
Kongfigurer alternativer for sikkerhet på arbeidsstasjonen (blandet modus)	19
Kongfigurer e-postvarsel (blandet modus)	20
Kongfigurer tilgang til SCIEX OS-programvaren	20
SCIEX OS Tillatelser	22
Om brukere og roller	29
Administrer brukere	39
Administrer roller	40
Eksporter og importer brukeradministrasjonsinnstillinger	41
Eksporter innstillinger for brukeradministrasjon	42
Importer brukeradministrasjonsinnstillinger	42

Innhold

Gjenopprett brukeradministrasjonsinnstillinger	42
Konfigurere tilgang til prosjekter og prosjektfiler	43
Prosjektmapper	43
Programvare-filtyper	43
Kapittel 5: Central Administrator Console	46
Bruker	46
Brukerutvalg	46
Brukerroller og tillatelser	47
Arbeidsgrupper	57
Opprette en arbeidsgruppe	57
Slette en arbeidsgruppe	58
Legg til brukere eller grupper i en arbeidsgruppe	58
Legg til arbeidsstasjoner i en arbeidsgruppe	59
Legg til prosjekter i en arbeidsgruppe	60
Administrer prosjekter	60
Om prosjekter og rotkataloger	61
Legg til en rotkatalog	61
Slette en prosjektkatalog	62
Legg til prosjekt	62
Legg til en undermappe	62
Arbeidsstasjoner	63
Legg til en arbeidsstasjon	63
Slette en arbeidsstasjon	64
Rapporter og sikkerhetsfunksjoner	64
Generere datarapporter	64
Eksporter CAC for brukeradministrasjon	64
Importer CAC for brukeradministrasjon	65
Gjenopprett CAC-programvareinnstillinger	65
Eksporter CAC brukeradministrasjonsinnstillinger	66
Importer CAC brukeradministrasjonsinnstillinger	66
Kapittel 6: Nettverksinnsamling	68
Om nettverksinnsamling	68
Fordelene ved å bruke nettverksinnsamling	68
Sikker nettverkskonto	68
Dataoverføringsprosess	70
Konfigurer nettverksinnsamling	71
Spesifiser en sikker nettverkskonto	71
Kapittel 7: Revisjon	72
Revisjonsspor	72
Revisjonskart	73
Oppsett av revisjonskart	74
Installerte revisjonskartmaler	75
Arbeid med revisjonskart	75
Revisjonskart for prosjekt	75
Revisjonskart for arbeidsstasjon	77

CAC Revisjonskart.....	79
Vise, søke, eksportere og skrive ut revisjonsspor.....	81
Vise revisjonssporoppføringer.....	81
Søke etter eller filtrere en revisjonsoppføring.....	82
Vise et arkivert revisjonsspor.....	82
Skrive ut et revisjonsspor.....	83
Eksporter revisjonssporoppføringer.....	83
Revisjonssporregistreringer.....	83
CAC Revisjonssporoppføringer.....	84
Revisjonssporarkiver.....	85
 Tillegg A: Windows-tillatelser.....	 86
 Tillegg B: Revisjonshendelser.....	 88
 Tillegg C: Tilordning av tillatelser mellom Analyst- og SCIEX OS-programvaren.....	 97
 Tillegg D: Sjekksum for datafiler.....	 104
Aktiver eller deaktiver datafilens sjekksumfunksjon.....	104
 Kontakt oss.....	 105
Adresser.....	105
Kundeopplæring.....	105
Online læresenter.....	105
SCIEX-støtte.....	105
Cybersikkerhet.....	106
Dokumentasjon.....	106

Informasjonen i denne håndboken er ment for to primære målgrupper:

- Laboratorieadministratoren, som tar seg av den daglige driften og bruken av SCIEX OS-programvaren og tilknyttet instrumentering fra et funksjonelt perspektiv.
- Systemadministratoren, som tar seg av systemsikkerhet og system- og dataintegritet.

Oversikt over sikkerhetskonfigurasjon

2

Denne delen beskriver hvordan tilgangskontroll- og revisjonskomponentene i SCIEX OS-programvaren fungerer sammen med Windows sine tilgangskontroll- og revisjonskomponenter. Det beskriver også hvordan du konfigurerer Windows-sikkerhet før du installerer SCIEX OS-programvaren.

Sikkerhet og overholdelse av forskrifter

SCIEX OS-programvaren leverer:

- Tilpassbar administrasjon for å oppfylle behovene til både forskning og forskriftsmessige krav.
- Sikkerhets- og revisjonsverktøy for å støtte overholdelse av 21 CFR del 11 for bruk av elektronisk journalføring.
- Fleksibel og effektiv styring av tilgang til kritiske funksjoner for massespektrometer.
- Kontrollert og revidert tilgang til vitale data og rapporter.
- Enkel sikkerhetsadministrasjon knyttet til Windows-sikkerhet.

Sikkerhetskrav

Sikkerhetskrav spenner fra relativt åpne miljøer, for eksempel forskningslaboratorier eller akademiske laboratorier, til de strengest regulerte, for eksempel forensiske laboratorier.

Sikkerhetskrav spenner fra relativt åpne miljøer, for eksempel forskningslaboratorier eller akademiske laboratorier, til de strengest regulerte, for eksempel kliniske laboratorier.

SCIEX OS-programvare og Windows-sikkerhet: Samarbeid

SCIEX OS-programvaren og NTFS (Windows New Technology File System) har sikkerhetsfunksjoner som er designet for å kontrollere system- og datatilgang.

Windows-sikkerhet sørger for det første beskyttelsesnivået ved å kreve at brukerne logger seg på nettverket ved hjelp av en unik brukeridentitet og et passord. Dette sikrer for at bare brukere som gjenkjennes av lokale sikkerhetsinnstillinger eller sikkerhetsinnstillinger for nettverk i Windows kan ha tilgang til systemene. For mer informasjon, se avsnittet: [Konfigurere Windows-sikkerhet](#).

SCIEX OS-programvaren har følgende sikre tilgangsmoduser:

- Blandet modus

Oversikt over sikkerhetskonnfigurasjon

- Integrert modus (standardinnstilling)

For mer informasjon om sikkerhetsmoduser og sikkerhetsinnstillinger, se avsnittet: [Konfigurer sikkerhetsmodusen](#).

SCIEX OS gir også for fullstendig konfigurerbare roller som er atskilt fra brukergruppene som er tilknyttet Windows. Gjennom bruk av roller kan laboratoriedirektøren styre funksjonsbasert tilgang til programvaren og massespektrometeret. For mer informasjon, se avsnittet: [Konfigurer tilgang til SCIEX OS-programvaren](#).

revisjonsspor i SCIEX OS-programvaren og Windows

Revisjonsfunksjonene i SCIEX OS-programvaren, sammen med de innebygde revisjonskomponentene i Windows, er avgjørende for opprettelse og styring av elektroniske registre.

SCIEX OS har et revisjonssporsystem for å oppfylle krav til elektroniske registre. Separat revisjonssporregistrering:

- Endringer i massekalibreringstabellen eller oppløsningstabellen, endringer i systemkonfigurasjon og sikkerhetshendelser.
- Opprettings- og modifiseringshendelser i prosjekter, tuning., batcher, data, prosesseringsmetoder og rapportmalfiler, åpning og lukking av moduler samt utskriftshendelser. Slettingshendelser registrert i revisjonssporet inkluderer sletting av roller og sletting av brukere i SCIEX OS-programvaren.
- Oppretting og modifisering av prøveinformasjonen, toppintegreringsparametere og innebygd behandlingsmetode i en resultattabell.

For en fullstendig liste over revisjonshendelser, se avsnittet: [Revisjonshendelser](#).

SCIEX OS-programvaren brukerprogramhendelseslogg for å fange opp informasjon om programvaredrift. Bruk denne loggen som et hjelpemiddel for feilsøking. Den inneholder detaljert informasjon om samhandlinger mellom massespektrometeret, apparatet og programvaren.

Windows vedlikeholder hendelseslogger som fanger opp en rekke sikkerhets-, system- og programrelaterte hendelser. I de fleste tilfeller er Windows-revisjon UTFormet for å fange opp eksepsjonelle hendelser, for eksempel en påloggingsfeil. Administratoren kan konfigurere dette systemet til å fange opp et bredt spekter av hendelser, for eksempel tilgang til bestemte filer eller Windows-administrasjonsaktiviteter. For mer informasjon, se avsnittet: [Systemrevisjoner](#).

Veiledning for kundesikkerhet: Sikkerhetskopier

Sikkerhetskopiering av kundedata er kundens ansvar. Selv om SCIEX service- og støttepersonell kan gi råd og anbefalinger om sikkerhetskopiering av kundedata, er det opp til kunden å sørge for at dataene sikkerhetskopies i henhold til kundens retningslinjer, behov og lovbestemte krav. Hyppigheten og dekningen av sikkerhetskopiering av kundedata bør stå i forhold til organisasjonens krav og hvor kritiske dataene som genereres er.

Kundene bør sørge for at sikkerhetskopier er funksjonelle, fordi sikkerhetskopier er en viktig del av den generelle dataadministrasjonen og avgjørende for gjenoppretting i tilfelle et ondsinnet angrep, maskinvarefeil eller programvarefeil. Ikke sikkerhetskopier datamaskinen under datainnsamlingen, ellers må det påses at filene som hentes, blir ignorert av sikkerhetskopieringsprogramvaren. Vi anbefaler på det sterkeste at du tar full sikkerhetskopi av datamaskinen før du installerer sikkerhetsoppdateringer eller UTFører reparasjoner på datamaskinen. Dette vil forenkle en tilbakeføring i det sjeldne tilfellet at en sikkerhetsoppdatering påvirker noen programfunksjonalitet.

21 CFR del 11

SCIEX OS-programvaren inneholder de tekniske kontrollene til å støtte 21 CFR del 11, med implementering av:

- Sikkerhet i blandet modus og integrert modus knyttet til Windows-sikkerhet.
- Kontrollert tilgang til funksjonalitet gjennom tilpassbare roller.
- Revisjonsspor for instrumentdrift, datainnsamling, datagjennomgang og generering av rapporter.
- Elektroniske signaturer ved bruk av en kombinasjon av bruker-ID og passord.
- Riktig konfigurasjon av Windows-operativsystemet.
- korrekte prosedyrer og opplæring i bedriften.

SCIEX OS-programvaren er UTFormet for bruk som en del av et system som er kompatibelt med 21 CFR del 11, og det kan konfigureres til å støtte samsvar med 21 CFR del 11. Hvorvidt bruken av SCIEX OS-programvaren er kompatibel med 21 CFR del 11, avhenger av bruken av den valgfrie SCIEX OS CFR-lisensen og konfigurasjonen av SCIEX OS-programvaren. Nødvendige retningslinjer og prosedyrer, og tilhørende opplæringskrav, må også være på plass i laboratoriet.

Valideringstjenester er tilgjengelige via SCIEX Professional Services. For mer informasjon, ta kontakt med complianceservices@sciex.com.

Merk: Ikke etterlat Instrument Settings Converter-programvaren på et validert system. Den er ment for den første overføringen av instrumentinnstillinger fra Analyst SCIEX OS-programvaren. Sørg for å fjerne Instrument Settings Converter-programvaren fra datamaskinen etter bruk.

Systemkonfigurasjon

Systemkonfigurasjon UTFøres vanligvis av nettverksadministratorer eller personer med rettigheter for nettverks- og lokal administrasjon.

Konfigurere Windows-sikkerhet

Dette avsnittet inneholder retningslinjer for konfigurasjon av Windows:

Oversikt over sikkerhetskonfigurasjon

- Følg disse retningslinjene for Windows-kontoer og passord:
 - Windows-passordet må endres hver 90. dag.
 - Windows-passordet kan ikke brukes på nytt i minst én etterfølgende periode. Det vil si at det ikke kan være det samme som det forrige passordet.
 - Windows-passordet må bestå av minst åtte tegn.
 - Windows-passordet må inneholde minst to av følgende fire krav for å oppfylle kompleksitetskravene:
 - Ett alfa-tegn med store bokstaver
 - Ett alfa-tegn med små bokstaver
 - Én numerisk verdi
 - Ett spesialtegn (for eksempel: ! @ # \$ % ^ &)
 - Windows-brukernavnet må ikke være **admin**, **Administrator** (**Administrator**) eller **demo**.
- Forsikre deg om at administratoren av SCIEX OS-programvaren har mulighet til å endre filtilatelser for SCIEX OS Data-mappen. Hvis denne mappen er på en lokal datamaskin, foreslår vi at programvareadministratoren er en del av den lokale administratorgruppen.
- Be nettverksadministratoren om å legge til en sikker nettverkskonto (SNA) på nettverksressursen for å sikre at alle brukere har nødvendig tilgang til ressurser for nettverksinnsamling. Denne kontoen må ha skrive-tilatelser for nettverksmappen som inneholder rotkatalogen. Den er definert som SNA i egenskapene for rotkatalogen.

Merk: Vi anbefaler at bibliotekfiler importeres fra en lokal stasjon.

Merk: For informasjon om Windows-tiltelsene som kreves for ulike brukerroller, se avsnittet: [Windows-tiltelser](#).

Brukere og grupper

SCIEX OS-programvaren bruker det brukernavnet og passordet som er registrert i den primære domenekontrollerens sikkerhetsdatabase eller Active Directory. Passord administreres ved hjelp av verktøyene i Windows. For mer informasjon om å legge til og konfigurere personer og roller, se avsnittet: [Konfigurer tilgang til SCIEX OS-programvaren](#).

Active Directory-støtte

Når du legger til brukere i Configuration-arbeidsområdet til SCIEX OS, angir du brukerkontoer i UPN-format (User Principal Name). Følgende versjoner av Active Directory støttes:

- Windows 2012-servere
- Windows 10-klienter, 64-biters klienter

Merk: SCIEX OS-programvaren er kun kompatibel med miljøer som bruker lokal Active Directory-lagring. Miljøer som bruker skylagring støttes ikke.

Windows-filsystem

I SCIEX OS-programvaren må filer og kataloger lagres på en harddiskpartisjon formatert som NTFS, som kan kontrollere og revidere tilgangen til SCIEX OS-programvarefiler. FAT-filsystemet kan ikke kontrollere eller revidere tilgangen til mapper eller filer, og er derfor ikke egnet for et sikkert miljø.

Fil- og mappetillatelser

For å administrere sikkerhet må administratoren av SCIEX OS-programvaren ha rett til å endre tillatelser for SCIEX OS Data-mappen. Tilgang må konfigureres av nettverksadministratoren.

For informasjon om Windows-tillatelsene som kreves for ulike brukerroller, se avsnittet: [Windows-tillatelser](#).

Merk: Vurder tilgangsnivået brukerne trenger til stasjonen, rotkatalogen og prosjektmappene på hver datamaskin. Konfigurer deling og tilknyttede tillatelser. For mer informasjon om fildeling, se Microsoft Windows-dokumentasjonen.

Merk: For å unngå problemer med tillatelser, anbefaler vi at bibliotekfiler importeres fra en lokal stasjon.

Merk: Programvaren antar at tillatelser for en prosjektmappe er arvet fra rotkatalogen.

For informasjon om filer og mappetillatelser i SCIEX OS-programvaren, se avsnittet: [tilgangskontroll](#).

Systemrevisjoner

Revisjonsfunksjonen til Windows-systemet kan aktiveres for å oppdage sikkerhetsbrudd eller systeminnbrudd. Revisjon kan settes til å registrere forskjellige typer systemrelaterte hendelser. For eksempel kan revisjonsfunksjonen aktiveres for å registrere ethvert mislykket eller vellykket påloggingsforsøk for å få tilgang til systemet, i hendelsesloggen.

Hendelseslogger

Windows Event Viewer registrerer de reviderte hendelsene i sikkerhetsloggen, systemloggen eller programloggen.

Tilpass hendelsesloggene som følger:

- Angi en passende størrelse på hendelsesloggen.
- Angi automatisk overskriving av gamle hendelser.

Oversikt over sikkerhetskonnfigurasjon

- Angi Windows-datamaskinens sikkerhetsinnstillinger.

En prosess med gjennomgang og lagring kan implementeres. For mer informasjon om sikkerhetsinnstillinger og revisjonsretningslinjer, se Windows-dokumentasjonen.

Windows-varsler

Hvis det oppstår et system- eller brukerproblem, kan du konfigurere nettverket til å sende en automatisk melding til en utpekt person, for eksempel systemadministratoren, på samme eller en annen datamaskin.

- På både sender- og mottakerdatamaskinen starter du Messenger-tjenesten i Windows Services-kontrollpanelet.
- På den sendende datamaskinen starter du varslingstjenesten i Windows Services-kontrollpanelet.

For mer informasjon om oppretting av et varslingsobjekt, se Windows-dokumentasjonen.

For SCIEX OS-programvaren kan elektronisk lisensiering være nodelåst eller serverbasert.

For Central Administrator Console (CAC)-programvaren er bare nodelåste lisenser tilgjengelige.

Aktiverings-ID kan være nødvendig for fremtidige service- eller støttesamtaler. Slik finner du aktiverings-ID-en til den nodelåste eller serverbaserte lisensen:

- I SCIEX OS-vinduet, åpne Configuration-arbeidsområdet, og klikk deretter på **Lisenser**.

Merk: Sørg for å fornye lisensen før den utløper. Lisensen for CAC-programvaren er en årlig lisens.

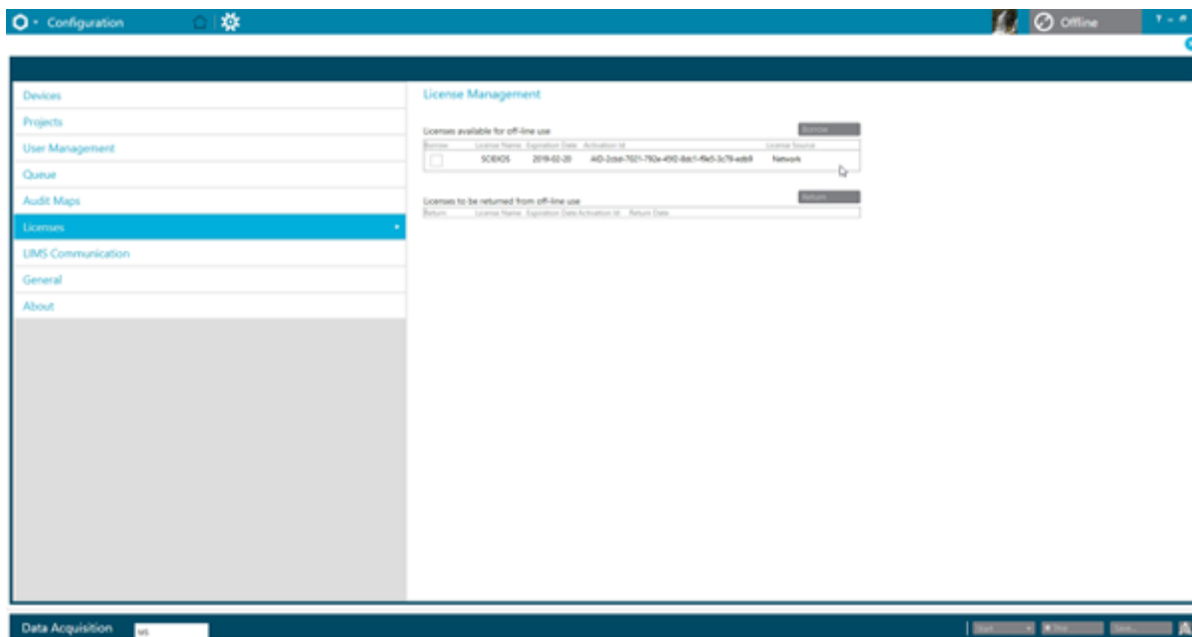
Lån en serverbasert elektronisk lisens

Det kreves en lisens for å bruke SCIEX OS. Hvis serverbasert lisensiering brukes, kan brukere som ønsker å jobbe frakoblet reservere en lisens i opptil 7 dager. I denne perioden er den lånte elektroniske lisensen dedikert til datamaskinen.

Merk: Denne prosedyren gjelder ikke for Central Administrator Console (CAC)-programvaren.

1. Åpne Configuration-arbeidsområdet.
2. Klikk på **Lisenser**.
Licenses available for off-line use-tabellen viser alle lisensene som er tilgjengelige for lån.

Figur 3-1: Lisensadministrasjon: Låne en lisens



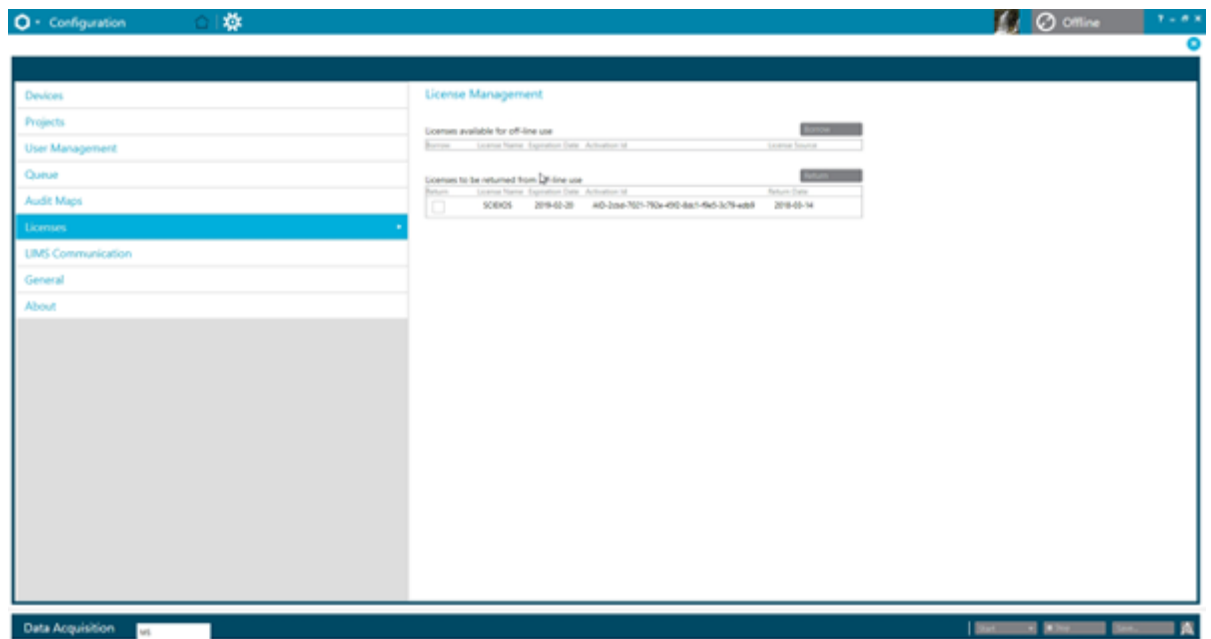
3. Velg lisensen som skal lånes, og klikk deretter på **Lån**.

Returner en serverbasert elektronisk lisens

Merk: Denne prosedyren gjelder ikke for Central Administrator Console (CAC)-programvaren.

1. Åpne Configuration-arbeidsområdet.
2. Klikk på **Lisenser**.
Licenses to be returned from off-line use-tabellen viser alle lisensene som er kvalifisert for retur, det vil si alle lisenser som er lånt av denne datamaskinen.

Figur 3-2: Lisensadministrasjon: Returner en lisens



3. Velg lisensen som skal returneres, og klikk deretter på **Retur**.

Denne delen beskriver hvordan du kontrollerer tilgangen til SCIEX OS-programvaren. Administratoren gjør følgende oppgaver for å kontrollere tilgangen til programvaren:

Merk: For å UTFøre oppgavene i denne delen må brukeren ha lokale administratorrettigheter for den arbeidsstasjonen som programvaren installeres på.

- Installer og konfigurer SCIEX OS-programvaren.
- Legge til og slette brukere og roller.
- Konfigurer tilgang til prosjektene og prosjektfilene i rotkatalogen.

Denne prosedyren gir instruksjoner for lokal administrasjon av SCIEX OS-programvaren. For sentralisert administrasjon av SCIEX OS-programvaren, se avsnittet: [Central Administrator Console](#).

Merk: Eventuelle endringer i SCIEX OS-konfigurasjonen trer i kraft etter at SCIEX OS er startet på nytt.

Plassering av sikkerhetsinformasjon

All sikkerhetsinformasjon lagres på den lokale datamaskinen, i mappen `C:\ProgramData\SCIEX\Clearcore2.Acquisition`, i en fil med navnet `Security.data`.

Arbeidsflyt for programvaresikkerhet

SCIEX OS-programvaren fungerer med revisjonskomponenter for sikkerhet, program og systemrevisjon i Windows Administrative Tools.

Konfigurer sikkerheten på følgende nivåer:

- Windows-autentisering: Tilgang til datamaskinen.
- Windows-autorisering: Tilgang til filer og mapper.
- SCIEX OS-programvareautentisering: Mulighet til å åpne SCIEX OS.
- SCIEX OS-programvareautentisering: Tilgang til funksjonalitet i SCIEX OS.

For listen over oppgaver for konfigurering av sikkerhet, se tabellen: [Tabell 4-1](#). For alternativene for å sette de ulike sikkerhetsnivåene, se tabellen: [Tabell 4-2](#).

Tabell 4-1: Arbeidsflyt for konfigurering av sikkerhet

Oppgave	Fremgangsmåte
Installer SCIEX OS-programvaren.	Se dokumentet: <i>SCIEX OS veiledning for programvareinstallasjon</i> .
Konfigurer tilgang til SCIEX OS-programvaren.	Se avsnittet: Konfigurer tilgang til SCIEX OS-programvaren .
Konfigurere Windows-filsikkerhet og NTFS.	Se avsnittet: Konfigurere tilgang til prosjekter og prosjektfiler .

Tabell 4-2: Alternativer for sikkerhetskongifurasjon

Alternativ	CFR 21 del 11
Windows-sikkerhet	
Konfigurere brukere og grupper (autentisering).	Ja
Aktivere Windows-revisjon og fil- og katalogrevisjon.	Ja
Angi filtillatelser (autorisering).	Ja
SCIEX OS-programvareinstallasjon	
Installer SCIEX OS-programvaren.	Ja
Åpne Event Viewer for å inspisere installasjonen.	Ja
Programvaresikkerhet	
Velge sikkerhetsmodus.	Ja
Konfigurer brukere og roller i SCIEX OS-programvaren.	Ja
Konfigurere e-postvarsling.	Ja
Opprett revisjonskartmaler, og konfigurer revisjonssporkart for prosjekter og arbeidsstasjoner.	Ja
Aktiver kontrollsumfunksjonen for <i>wiff</i> -filer.	Ja
Vanlige oppgaver	
Legg til nye prosjekter.	Ja

Installer programvaren SCIEX OS

Før du installerer SCIEX OS-programvaren, må du lese disse dokumentene, som er tilgjengelige på DVD-en for programvareinstallasjon eller nedlastingspakken for Internett: *Veiledning for programvareinstallasjon* og *Versjonsmerknader*. Du må også forstå forskjellen mellom en arbeidsstasjon for behandling og en arbeidsstasjon for innsamling, og deretter gjennomføre riktig installasjonssekvens.

Systemkrav

For minimums installasjonskrav, se dokumentet: *Veiledning for programvareinstallasjon*.

Forhåndsinnstilte revisjonsalternativer

For en beskrivelse av installerte revisjonskart, se avsnittet: [Installerte revisjonskartmaler](#). Etter installasjon kan administratoren av SCIEX OS-programvaren opprette egendefinerte revisjonskart og tilordne et annet revisjonskart i Configuration-arbeidsområdet.

Konfigurer sikkerhetsmodusen

Denne delen beskriver Security Mode-alternativene som finnes på siden User Management i Configuration-arbeidsområdet.

Integrated Mode (Integrert modus): Hvis brukeren som for øyeblikket er logget på Windows, er definert som bruker i -programvaren, har brukeren tilgang til SCIEX OS-programvaren.

Mixed Mode (Blandet modus): Brukere logger på Windows og programvaren separat. Påloggingsinformasjonen som brukes til å logge på Windows, trenger ikke være den samme som påloggingsinformasjonen som brukes til å logge på SCIEX OS. Bruk denne modusen for å tillate en gruppe brukere å logge på Windows med det samme settet med påloggingsinformasjon, men krever at hver bruker logger på programvaren med unike påloggingsinformasjon. Disse unike legitimasjonene kan tilordnes en spesifisert rolle på samme måte som i integrert modus.

Hvis **Mixed Mode (Blandet modus)** er valgt, er **Skjermlås** og **Automatisk utlogging**-alternativene tilgjengelige.

Skjermlås og Automatisk utlogging: Av sikkerhetshensyn kan dataskjermen stilles inn til å låses etter en definert periode med inaktivitet. En automatisk avloggingstimer kan også stilles inn for å lukke programvaren etter at den har vært låst i en spesifisert periode. **Skjermlås og Automatisk utlogging** er bare tilgjengelige dersom **Mixed Mode (Blandet modus)** er valgt.

Merk: Når skjermen låses, fortsetter innhenting og behandlingen. Automatisk utlogging vil ikke skje hvis behandlingen pågår eller hvis resultattabellen ikke er lagret. Når brukeren er logget av med tvungen avlogging, stopper all behandling, og alle ulagrede data går tapt. Innhenting fortsetter etter at brukeren er logget av automatisk eller manuelt.

Varslinger: Programvaren kan konfigureres til å automatisk sende en e-postvarsling etter et konfigurerbart antall påloggingsfeil i løpet av en konfigurerbar periode, for å varsle om forsøk på å få tilgang til systemet av uautoriserte brukere. Antall påloggingsfeil kan være fra 3 til 7, og perioden kan være fra 5 minutter til 24 timer.

Merk: For arbeidsgrupper som administreres av CAC-programvaren Central Administrator Console (CAC) kan ikke sikkerhetsmodusen administreres sammen med SCIEX OS-programvaren.

Velge sikkerhetsmodus

1. Åpne Configuration-arbeidsområdet.
2. Klikk på **Brukeradministrasjon**.
3. Klikk på **Security Mode (Sikkerhetsmodus)**-fanen.
4. Velg **Integrated Mode (Integrert modus)** eller **Mixed Mode (Blandet modus)**. Se avsnittet: [Konfigurer sikkerhetsmodusen](#).
5. Klikk på **Save (Lagre)**.
En bekreftelsesdialogboks vises.
6. Klikk på **OK**.

Konfigurer alternativer for sikkerhet på arbeidsstasjonen (blandet modus)

Forutsetninger for prosedyrer
• Sett sikkerhetsmodusen til blandet modus. Se avsnittet: Konfigurer sikkerhetsmodusen.

Hvis Blandet modus er valgt, kan funksjonene Screen Lock og Auto Logoff konfigureres.

1. Åpne Configuration-arbeidsområdet.
2. Klikk på **Brukeradministrasjon**.
3. Åpne Security Mode-fanen.
4. Følg disse trinnene for å konfigurere skjermlåsfunksjonen:
 - a. Velg **Skjermlås**.
 - b. I **Vent**-feltet angir du et klokkeslett i minutter.
Hvis arbeidsstasjonen er inaktiv i så lang tid, låses den automatisk. Den påloggede brukeren kan låse opp arbeidsstasjonen ved å skrive inn riktig legitimasjon, eller administratoren kan logge av brukeren.
5. Følg disse trinnene for å konfigurere funksjonen for automatisk pålogging:
 - a. Velg **Automatisk utlogging**.
 - b. I **Vent**-feltet angir du et klokkeslett i minutter. Hvis arbeidsstasjonen er låst i så lang tid, enten automatisk eller manuelt, blir den påloggede brukeren logget av. All behandling stoppes. Imidlertid fortsetter anskaffelse.
6. Klikk på **Save (Lagre)**.
En bekreftelsesdialogboks åpnes.
7. Klikk på **OK**.

Konfigurer e-postvarsel (blandet modus)

Forutsetninger for prosedyrer

- | |
|---|
| <ul style="list-style-type: none">• Sett sikkerhetsmodusen til blandet modus. Se avsnittet: Konfigurer sikkerhetsmodusen. |
|---|

Programvaren kan konfigureres til å sende en e-postmelding etter et konfigurerbart antall påloggingsfeil i løpet av en konfigurerbart periode. Antall påloggingsfeil kan være fra 3 til 7, og perioden fra 5 minutter til 24 timer.

Datamaskinen med installert programvare må kunne kommunisere med en SMTP-server med en åpen port.

1. Åpne Configuration-arbeidsområdet.
2. Klikk på **Brukeradministrasjon**.
3. Åpne Security Mode-fanen.
4. Velg avmerkingsboksen **Send e-postmeldinger etter**, og angi deretter hvor mange påloggingsfeil i løpet av hvilken periode, i minutter, som vil generere et e-postvarsel.

Tips! Fjern merket i avmerkingsboksen **Send e-postmeldinger etter** for å deaktivere varsel.

5. Skriv inn navnet på SMTP-serveren i **SMTP-server**-feltet.

Merk: SMTP-kontoen sender e-post til e-postserveren. SMTP-serveren er definert i bedriftens e-postprogram.

6. I **Portnummer**-feltet skriver du inn nummeret til den åpne porten. Klikk på **Bruk standard** for å sette inn standard portnummer, 25.
7. I **To**-feltet skriver du inn e-postadressen som meldingen skal sendes til. For eksempel: username@domain.com.
8. I **From**-feltet skriver du inn e-postadressen som skal vises i **From**-meldingsfeltet.
9. Skriv emnet for meldingen i feltet **Emne**.
10. I **Melding**-feltet skriver du inn teksten som skal inkluderes i meldingen.
11. Klikk på **Save (Lagre)**.
En bekreftelsesdialogboks åpnes.
12. Klikk på **OK**.
13. Klikk på **Send test-e-post** for å sjekke konfigurasjonen.

Konfigurer tilgang til SCIEX OS-programvaren

Gjør følgende før du konfigurerer sikkerhet:

- Fjern alle unødvendige brukere og brukergrupper, som f.eks. replikator, privilegert bruker og sikkerhetskopioperatør, fra den lokale datamaskinen og nettverket.

Merk: Hver SCIEX-datamaskin er konfigurert med et lokal administrator-kontonivå, **abservice**. Denne kontoen brukes av SCIEX-service og teknisk støtte for å installere, vedlikeholde og støtte systemet. Ikke fjern eller deaktiver denne kontoen. Hvis kontoen må fjernes eller deaktiveres, utarbeider du en alternativ plan for SCIEX-tilgang, og kommuniserer den til den lokale FSE.

- Legg til brukergrupper som inneholder grupper som har ikke-administrative oppgaver.
- Konfigurer systemtillatelser.
- Lag egnede prosedyrer og kontoretningslinjer for brukere i grupperetningslinjer.

Se Windows-dokumentasjonen for mer informasjon om følgende:

- Brukere og grupper og Active Directory-brukere.
- Retningslinjer for passord og retningslinjer for kontolåsing for brukerkontoer.
- Retningslinjer for brukerrettigheter.

Når brukere jobber i et Active Directory-miljø, påvirker innstillingene for grupperetningslinjer for Active Directory datamaskinens sikkerhet. Diskuter grupperetningslinjer med Active Directory-administratoren som en del av en omfattende distribusjon av SCIEX OS-programvaren.

SCIEX OS Tillatelser

Figur 4-1: Siden User Management

Configuration

Devices

Projects

User Management

Queue

Print Templates

Audit Maps

Licenses

LIMS Communication

General

Software Updates

Service and Support

CAC

About

Users

Roles

Security

User Roles and Permission Categories

Permission	Administrator	Method Developer	Analyst	Reviewer
▼ Batch				
Submit unlocked methods	☒	☒	☒	☐
Open	☒	☒	☒	☒
Save as	☒	☒	☒	☐
Submit	☒	☒	☒	☐
Save	☒	☒	☒	☐
Save ion reference table	☒	☒	☒	☐
Add data sub-folders	☒	☒	☒	☐
Configure Decision Rules	☒	☒	☒	☐
Overwrite a batch	☒	☒	☒	☐
Submit batch before save	☒	☒	☒	☐
▼ Configuration				
General tab	☒	☒	☐	☐
General: change regional setting	☒	☒	☐	☐
General: full screen mode	☒	☒	☐	☐
LIMS communication tab	☒	☒	☐	☐
General: Stop Windows services	☒	☐	☐	☐
Audit maps tab	☒	☐	☐	☐

Tabell 4-3: Tillatelser

Tillatelse	Beskrivelse
Batch (Parti)	
Send inn ulåste metoder	Sende inn batcher som inneholder ulåste metoder.
Open (Åpne)	Åpne eksisterende batcher.
Save As (Lagre som)	Lagre batcher med et nytt navn.
Submit (Send inn)	Sende inn batcher.
Save (Lagre)	Lagre en batch og overskriv det lagrede innholdet.
Lagre ionereferansetabell	Rediger ionereferansetabellen.

Tabell 4-3: Tillatelser (fortsatt)

Tillatelse	Beskrivelse
Legg til undermapper for data	Opprett undermapper for datalagring.
Konfigurer beslutningsregler	Legge til og endre beslutningsregler.
Overskriv batch	Lagre en batch med samme navn og overskriv det lagrede innholdet.
Send inn batch før lagring	Send inn en batch som ikke er lagret.
Konfigurasjon	
Generell fane	Åpne siden General i Configuration-arbeidsområdet.
Generelt: endre regional innstilling	Bruk de aktive systemregionale innstillingene på SCIEX OS-programvaren.
Generelt: fullskjermmodus	Aktiver og deaktiver fullskjermmodus.
Generelt: Stopp Windows-tjenester	Aktiverer eller deaktiverer alternativet Windows-innstillinger .
LIMS kommunikasjonsfane	Åpne siden LIMS Communication i Configuration-arbeidsområdet.
Fane for revisjonskart	Åpne siden Audit Maps i Configuration-arbeidsområdet.
Kø-fane	Åpne siden Queue i Configuration-arbeidsområdet.
Kø: instrumentets inaktive tid	Still inn instrumentets tomgangstid.
Kø: maks. antall innsamlede prøver	Angi maksimalt antall innhentede prøver som er tillatt.
Kø: andre køinnstillinger	Konfigurer andre køinnstillinger.
Prosjekter-fane	Åpne siden Projects i Configuration-arbeidsområdet.
Prosjekter: opprett prosjekt	Opprett prosjekter.
Prosjekter: bruk en revisjonskartmal på et eksisterende prosjekt	Bruk et revisjonskart på et prosjekt.
Prosjekter: opprett rotkatalog	Opprett en rotkatalog for prosjektlagring.
Prosjekter: angi gjeldende rotkatalog	Endre rotkatalogen for et prosjekt.

Tabell 4-3: Tillatelser (fortsett)

Tillatelse	Beskrivelse
Prosjekter: spesifiser nettverkslegitimasjon	Angi en sikker nettverkskonto (SNA) som skal brukes under nettverksinnhenting hvis brukeren som er logget på, ikke har tilgang til nettverksressursen.
Prosjekter: Aktiver kontrollsumskrivning for oppretting av wiff-data	Konfigurer programvaren til å skrive kontrollsummer til <i>wiff</i> -datafiler.
Prosjekter: tøm rotkatalog	Slett en rotkatalog fra listen.
Enhetsfane	Åpne siden Devices i Configuration-arbeidsområdet.
Brukeradministrasjon-fane	Åpne siden User Management i Configuration-arbeidsområdet.
Tving avlogging av bruker	Tving en bruker som er logget på SCIEX OS-programvaren til å logge av.
CAC-fane ¹	Åpne siden CAC i Configuration-arbeidsområdet.
Fanen utskriftsmal:	Åpne Print Templates-fanen i arbeidsområdet Configuration.
Utskriftsmaler: Opprett og endre utskriftsmaler	Lag nye utskriftsmaler eller endre lagrede utskriftsmaler.
Utskriftsmaler: Angi standard utskriftsmal	Gjør den aktive utskriftsmalen til standard for det aktive prosjektet.
Utskriftsmaler: Bruk gjeldende mal på alle prosjekter i rotkatalogen	Legg til utskriftsmalen i listen over tilgjengelige utskriftsmaler for valgte prosjekter i en valgt rotkatalog.
Hendelseslogg	
Tilgang til arbeidsområdet for hendelseslogg	Åpne Event Log-arbeidsområdet.
Arkiver logg	Arkiver loggene i Event Log arbeidsområdet.
Revisjonsspor	
Tilgang til arbeidsområdet for revisjonsspor	Åpne Audit Trail-arbeidsområdet.
Vis aktivt revisjonskart	Se det aktive revisjonskartet for en arbeidsstasjon eller et prosjekt i arbeidsområdet Revisjonsspor.
Skriv ut/eksporter revisjonsspor	Skriv ut eller eksporter revisjonssporet.
Datainnsamlingspanel	

¹ I versjon 3.1 ble tillatelsen **Aktiver sentraladministrasjon** omdøpt til **CAC**. CAC-siden i Configuration-arbeidsområdet kan brukes til å konfigurere sentral administrasjon av SCIEX OS-programvaren.

Tabell 4-3: Tillatelser (fortsatt)

Tillatelse	Beskrivelse
Start	Start innsamling i ruten Data Acquisition.
Stopp	Stopp innhenting i ruten Data Acquisition.
Save (Lagre)	Lagre innhentede data med et annet filnavn i ruten Data Acquisition.
MS & LC-metode	
Tilgangsmetode for arbeidsområde	Åpne arbeidsområdene MS Method og LC Method.
Nytt	Opprett MS- og LC-metoder.
Open (Åpne)	Åpne MS- og LC-metoder.
Save (Lagre)	Lagre en metode og overskriv det lagrede innholdet.
Save As (Lagre som)	Lagre metodene med et nytt navn.
Låse-/opplåsningsmetode	Lås metoder for å forhindre redigering, og låse opp metoder.
Overwrite acquisition methods (Overskrive innsamlingsmetoder)	Lagre en innsamlingsmetode med samme navn, og overskriv det lagrede innholdet.
Kø	
Administrer	Åpne Queue-arbeidsområdet.
Start/Stopp	Start eller stopp køen.
Print (Skriv ut)	Skriv ut køen.
Rediger prøve	Endre navnet eller datafilen for en prøve.
Bibliotek	
Tilgang til bibliotekets arbeidsområde	Åpne Library-arbeidsområdet. Gjelder ikke for kvantifiseringsarbeidsflyten.
MS tune	
Tilgang til MS Tune-arbeidsområdet	Åpne MS Tune-arbeidsområdet.
Avansert MS-tuning	TOF-systemer: Få tilgang til de avanserte justeringsalternativene, som inkluderer Detektoroptimalisering, Positiv TOF-tuning, Negativ TOF-tuning, Positiv Q1 enhetstuning, Negativ Q1 enhetstuning, Positiv Q1 høy tuning, og Negativ Q1 høy tuning.
Avansert feilsøking	Åpne dialogboksen Advanced Troubleshooting.

Tabell 4-3: Tillatelser (fortsett)

Tillatelse	Beskrivelse
Hurtig statuskontroll	TOF-systemer: Utfør Positiv hurtigstatuskontroll og Negativ hurtigstatuskontroll .
Gjenopprett instrumentdata	Gjenopprett tidligere lagrede justeringsinnstillinger.
Analyse	
Nye resultater	Opprette resultattabeller.
Opprett behandlingsmetoder	Opprette behandlingsmetoder.
Endre behandlingsmetode	Endre behandlingsmetoder.
Allow Export and Create Report of unlocked Results Table (Tillat eksport og opprett rapport om ulåste resultattabeller)	Hvis resultattabellen ikke er låst, kan du eksportere eller opprette en rapport fra en resultattabell eller statistikktabell.
Lagre resultater for automatiseringsbatch	Lagre resultattabeller som ble opprettet automatisk i arbeidsområdet Batch. Denne tillatelsen kreves for automatisk behandling under innsamling.
Change default quantitation method integration algorithm (Endre standardalgoritme for integrering av) kvantifiseringsmetoder	Endre integrasjonsalgoritmen i prosjektets standardinnstillinger.
Change default quantitation method integration parameters (Endre standardparametre for integrering av kvantifiseringsmetoder)	Endre integreringsparameterne i prosjektets standardinnstillinger.
Aktiver prosjektmodifisert toppadvarsel	Aktiver den endrede egenskapen for toppadvarsel for et prosjekt.
Legg til prøver	Legg til prøver i resultattabellen.
Fjern valgte prøver	Fjern prøver fra resultattabellen.
Eksporter, importer eller fjern ekstern kalibrering	Eksporter, importer eller fjern eksterne kalibreringer.
Endre prøvenavn	Endre prøvenavnet i resultattabellen.

Tabell 4-3: Tillatelser (fortsett)

Tillatelse	Beskrivelse
Endre prøvetype	Endre prøvetypen i resultattabellen. Gyldige prøvetyper inkluderer standard, kvalitetskontroll (QC) og ukjent.
Endre prøve-ID	Endre prøve-ID i resultattabellen.
Endre faktisk konsentrasjon	Endre den faktiske konsentrasjonen av standard- og QC-prøvene i resultattabellen.
Endre fortynningsfaktor	Endre fortynningsfaktoren i resultattabellen.
Endre kommentarfelt	Endre følgende kommentarfelt: • Component Comment • IS Comment • IS Peak Comment • Peak Comment • Sample Comment (Kommentar for prøven)
Aktiver manuell integrering	Utfør en manuell integrering.
Sett topp til 'Ikke funnet'	Angi en topp til Ikke funnet .
Inkluder eller ekskluder en topp fra resultattabellen	Inkluder eller ekskluder en topp fra resultattabellen.
Regresjonsalternativer	Endre regresjonsalternativene i ruten Calibration Curve.
Endre integreringsparametre for resultattabell for et enkelt kromatogram	Endre integrasjonsparametere for et enkelt kromatogram i ruten Peak Review.
Endre kvantifiseringsmetode for resultattabell-komponenten	Rediger den innebygde behandlingsmetoden, velg en annen behandlingsmetode for en komponent i ruten Peak Review med Oppdater behandlingsmetode for komponent eller Oppdater behandlingsmetode for gruppe -alternativet, eller endre navnet på en intern standard i Results Table.
Opprett nye innstillinger for metrisk diagram	Opprett nye metriske diagrammer og endre innstillingene.
Legg til egendefinerte kolonner	Legge til egendefinerte kolonner i en resultattabell.
Angi tittelformat for gjennomgang av topper	Endre tittelen på gjennomgangen av topper.
Remove custom column (Fjern egendefinert kolonne)	Fjern egendefinerte kolonner fra en resultattabell.

Tabell 4-3: Tillatelser (fortsett)

Tillatelse	Beskrivelse
Visningsinnstillinger for resultattabell	Endre kolonnene som vises i resultattabellen.
Lås resultattabell	Lås en resultattabell for å forhindre redigering.
Lås opp resultattabell	Lås opp en resultattabell for å la endringer bli gjort.
Merk resultatfilen som gjennomgått og lagre	Merk resultatfilen som gjennomgått, og lagre den.
Endre rapportmal	Endre logoen eller dimensjonene til en rapportmal.
Overfør resultater til LIMS	Last opp resultater til et LIMS-system (Laboratory Information Management System).
Endre strekkodekolonne	Endre Barcode -kolonnen i en resultattabell.
Endre sammenligningsprøvetildeling	Endre sammenligningsprøven som er angitt i Comparison -kolonnen i resultattabellen.
Legg til MSMS-spektra i biblioteket	Legg til MS/MS-spektrene i et bibliotek. Gjelder ikke for kvantifiseringsarbeidsflyten.
Prosjektets standardinnstillinger	Endre prosjektets standardinnstillinger for kvantitativ og kvalitativ behandling.
Opprett rapport i alle formater	Opprett rapporter i alle formater. Brukere uten denne tillatelsen kan bare opprette rapporter i PDF-format.
Rediger parametere for flaggingskriterier	Endre flaggingsparameterne i en behandlingsmetode.
Parameterendring for automatisk fjerning av avvik	Endre parameterne for automatisk fjerning av avvik.
Aktiver automatisk fjerning av avvik	Endre behandlingsmetoden for å slå på funksjonen for automatisk fjerning av avvik.
Oppdater behandlingsmetode via FF/LS	Bruk Formelfinner og Bibliotekssøk til å oppdatere behandlingsmetoder. Gjelder ikke for kvantifiseringsarbeidsflyten.
Oppdater resultater via FF/LS	Bruk Formula Finder og bibliotekssøk for å oppdatere resultatene. Gjelder ikke for kvantifiseringsarbeidsflyten.
Aktiver gruppering etter addukt-funksjonalitet	Oppdater behandlingsmetoden for å bruke funksjonen gruppering etter addukt.
Bla etter filer	Bla utenfor den lokale datamappen.
Aktiver standardtilføyelse	Oppdater behandlingsmetoden for å slå på standard tilleggsfunksjon.

Tabell 4-3: Tillatelser (fortsatt)

Tillatelse	Beskrivelse
Angi prosentregel for manuell integrering	Endre Manuell integrering %-parameteren.
Vekt/volum	Lar brukeren endre Weight/Volume (Vekt/volum) -feltet.
Overskriv en resultattabell	Lagre en resultattabell med samme navn, og skriv over det lagrede innholdet.
Merk resultatfilen som godkjent og lagre	Lar brukeren merke en resultatfil som godkjent og lagre den med Results > Merk resultatfilen som godkjent og lagre -kommandoen.
Sentral overvåking	
Fanen tilgangskø	Åpne Sentral overvåking -arbeidsområdet.
Utskriftskø	Skriv ut køen.
Start/stopp kø	Start eller stopp køen.
Utforsker	
Tilgang til arbeidsområde for UTForsker	Åpne Explorer-arbeidsområdet.
Export (Eksporter)	Eksporter data fra Explorer-arbeidsområdet.
Print (Skriv ut)	Skriv ut data i Explorer-arbeidsområdet.
Options (Alternativer)	Endre alternativene for Explorer-arbeidsområdet.
Kalibrer på nytt	Kalibrere prøver og spektra i Explorer-arbeidsområdet igjen. Gjelder ikke for kvantifiseringsarbeidsflyten.
Bla etter filer	Bla utenfor det aktive prosjektet.

Om brukere og roller

I SCIEX OS-programvaren kan administratoren legge til Windows-brukere og -grupper i databasen for brukeradministrasjon. For å få tilgang til programvaren må brukerne være i databasen for brukeradministrasjon eller være medlem av en gruppe i databasen.

Brukere kan tilordnes én eller flere av de forhåndsinnstilte rollene som vises i følgende tabell, eller til egendefinerte roller, om nødvendig. Funksjonene som en bruker har tilgang til, er spesifisert av roller. De forhåndsinnstilte rollene kan ikke slettes, og deres tillatelser kan ikke endres.

Merk: For arbeidsgrupper som administreres av Central Administrator Console (CAC)-programvaren, leses bare User Management-sidene.

Tabell 4-4: Forhåndsinnstilte roller

Role (Rolle)	Typiske oppgaver
Administrator (Administrator)	• Administrerer systemet • Konfigurerer sikkerhet
Metodeutvikler	• Oppretter metoder • Kjører batcher • Analyserer data for bruk av brukeren
Analyst	• Kjører batcher • Analyserer data for bruk av brukeren
Reviewer (Den som utfører gjennomgang)	• Går gjennom data • Går gjennom revisjonsspor • Går gjennom kvantifiseringsresultater

Tabell 4-5: Forhåndsinnstilte tillatelser

Tillatelse	Administrator (Administrator)	Metodeutvikler	Analyst	Reviewer (Den som utfører gjennomgang)
Batch (Parti)				
Send inn ulåste metoder	✓	✓	✓	X
Open (Åpne)	✓	✓	✓	✓
Save As (Lagre som)	✓	✓	✓	X
Submit (Send inn)	✓	✓	✓	X
Save (Lagre)	✓	✓	✓	X
Lagre ionereferansetabell	✓	✓	✓	X
Legg til undermapper for data	✓	✓	✓	X
Konfigurer beslutningsregler	✓	✓	✓	X

Tabell 4-5: Forhåndsinnstilte tillatelser (fortsett)

Tillatelse	Administrator (Administrator)	Metodeutvikler	Analyst	Reviewer (Den som utfører gjennomgang)
Overskriv batch	✓	✓	✓	X
Send inn batch før lagring	✓	✓	✓	✓
Konfigurasjon				
Generell fane	✓	✓	X	X
Generelt: endre regional innstilling	✓	✓	X	X
Generelt: fullskjermmodus	✓	✓	X	X
Generelt: Stopp Windows-tjenester	✓	X	X	X
LIMS kommunikasjons fane	✓	✓	X	X
Fane for revisjonskart	✓	X	X	X
Kø-fane	✓	✓	✓	✓
Kø: instrumentets inaktive tid	✓	✓	X	X
Kø: maks. antall innsamlede prøver	✓	✓	X	X
Kø: andre køinnstillinger	✓	✓	X	X
Prosjekter-fane	✓	✓	✓	✓
Prosjekter: opprett prosjekt	✓	✓	✓	X
Prosjekter: bruk en revisjonskartmal på et	✓	X	X	X

Tabell 4-5: Forhåndsinnstilte tillatelser (fortsett)

Tillatelse	Administrator (Administrator)	Metodeutvikler	Analyst	Reviewer (Den som utfører gjennomgang)
eksisterende prosjekt				
Prosjekter: opprett rotkatalog	✓	X	X	X
Prosjekter: angi gjeldende rotkatalog	✓	X	X	X
Prosjekter: spesifiser nettverkslegitimasjon	✓	X	X	X
Prosjekter: Aktiver kontrollsumskrivning for oppretting av wiff-data	✓	X	X	X
Prosjekter: tøm rotkatalog	✓	X	X	X
Enhetsfane	✓	✓	✓	X
Brukeradministrasjon-fane	✓	X	X	X
Tving avlogging av bruker	✓	X	X	X
CAC-fane ¹	✓	X	X	X
Fanen utskriftsmal:	✓	✓	X	X
Utskriftsmaler: Opprett og endre utskriftsmaler	✓	✓	X	X
Utskriftsmaler: Angi standard utskriftsmal	✓	✓	X	X

¹ I versjon 3.1 ble tillatelsen **Aktiver sentraladministrasjon** omdøpt til **CAC**. CAC-siden i Configuration-arbeidsområdet kan brukes til å konfigurere sentral administrasjon av SCIEX OS-programvaren.

Tabell 4-5: Forhåndsinnstilte tillatelser (fortsett)

Tillatelse	Administrator (Administrator)	Metodeutvikler	Analyst	Reviewer (Den som utfører gjennomgang)
Utskriftsmaler: Bruk gjeldende mal på alle prosjekter i rotkatalogen	✓	X	X	X
Hendelseslogg				
Tilgang til arbeidsområdet for hendelseslogg	✓	✓	✓	✓
Arkivlogg	✓	✓	✓	✓
Revisjonsspor				
Tilgang til arbeidsområdet for revisjonsspor	✓	✓	✓	✓
Vis aktivt revisjonskart	✓	✓	✓	✓
Skriv ut/ eksporter revisjonsspor	✓	✓	✓	✓
Datainnsamlingspanel				
Start	✓	✓	✓	X
Stopp	✓	✓	✓	X
Save (Lagre)	✓	✓	✓	X
MS & LC-metode				
Tilgangsmetode for arbeidsområde	✓	✓	✓	✓
Nytt	✓	✓	X	X
Open (Åpne)	✓	✓	✓	✓
Save (Lagre)	✓	✓	X	X
Save As (Lagre som)	✓	✓	X	X

Tabell 4-5: Forhåndsinnstilte tillatelser (fortsett)

Tillatelse	Administrator (Administrator)	Metodeutvikler	Analyst	Reviewer (Den som utfører gjennomgang)
Låse-/ opplåsningsmetode	✓	✓	X	X
Overwrite acquisition methods (Overskrive innsamlingsmetoder)	✓	✓	X	X
Kø				
Administrer	✓	✓	✓	X
Start/Stopp	✓	✓	✓	X
Print (Skriv ut)	✓	✓	✓	✓
Rediger prøve	✓	✓	X	X
Bibliotek				
Tilgang til bibliotekets arbeidsområde	✓	✓	✓	✓
MS tune				
Tilgang til MS Tune- arbeidsområdet	✓	✓	✓	X
Avansert MS- tuning	✓	✓	X	X
Avansert feilsøking	✓	✓	X	X
Hurtig statuskontroll	✓	✓	✓	X
Gjenopprett instrumentdata	✓	✓	X	X
Analyse				
Nye resultater	✓	✓	✓	X

Tabell 4-5: Forhåndsinnstilte tillatelser (fortsett)

Tillatelse	Administrator (Administrator)	Metodeutvikler	Analyst	Reviewer (Den som utfører gjennomgang)
Opprett behandlingsmetoder	✓	✓	✓	X
Endre behandlingsmetode	✓	✓	X	X
Allow Export and Create Report of unlocked Results Table (Tillat eksport og opprett rapport om ulåste resultattabeller)	✓	X	X	X
Lagre resultater for automatiseringsbatch	✓	✓	✓	X
Change default quantitation method integration algorithm (Endre standardalgoritme for integrering av) kvantifiseringsmetoder	✓	✓	X	X
Change default quantitation method integration parameters (Endre standardparametre for integrering av kvantifiseringsmetoder)	✓	✓	X	X

Tabell 4-5: Forhåndsinnstilte tillatelser (fortsett)

Tillatelse	Administrator (Administrator)	Metodeutvikler	Analyst	Reviewer (Den som utfører gjennomgang)
Aktiver prosjektmodifisert toppadvarsel	✓	X	X	X
Legg til prøver	✓	✓	✓	X
Fjern valgte prøver	✓	✓	✓	X
Eksporter, importer eller fjern ekstern kalibrering	✓	✓	✓	X
Endre prøvenavn	✓	✓	✓	X
Endre prøvetype	✓	✓	✓	X
Endre prøve-ID	✓	✓	✓	X
Endre faktisk konsentrasjon	✓	✓	✓	X
Endre fortynningsfaktor	✓	✓	✓	X
Endre kommentarfelt	✓	✓	✓	X
Aktiver manuell integrering	✓	✓	✓	X
Sett topp til 'Ikke funnet'	✓	✓	✓	X
Inkluder eller ekskluder en topp fra resultattabellen	✓	✓	✓	X
Regresjonsalternativer	✓	✓	✓	X
Endre integreringsparametre for resultattabell for et enkelt kromatogram	✓	✓	✓	X

Tabell 4-5: Forhåndsinnstilte tillatelser (fortsett)

Tillatelse	Administrator (Administrator)	Metodeutvikler	Analyst	Reviewer (Den som utfører gjennomgang)
Endre kvantifiseringsmetode for resultattabell-komponenten	✓	✓	✓	X
Opprett nye innstillinger for metrisk diagram	✓	✓	✓	✓
Legg til egendefinerte kolonner	✓	✓	✓	X
Angi tittelformat for gjennomgang av topper	✓	X	X	X
Remove custom column (Fjern egendefinert kolonne)	✓	✓	X	X
Visningsinnstillinger for resultattabell	✓	✓	✓	✓
Lås resultattabell	✓	✓	✓	✓
Lås opp resultattabell	✓	X	X	X
Merk resultatfilen som gjennomgått og lagre	✓	X	X	✓
Endre rapportmal	✓	✓	X	X
Overfør resultater til LIMS	✓	✓	✓	X
Endre strekkodekolonne	✓	✓	X	X

Tabell 4-5: Forhåndsinnstilte tillatelser (fortsett)

Tillatelse	Administrator (Administrator)	Metodeutvikler	Analyst	Reviewer (Den som utfører gjennomgang)
Endre sammenligningsprøvetildeling	✓	✓	X	X
Legg til MSMS-spektra i biblioteket	✓	✓	X	X
Prosjektets standardinnstillinger	✓	✓	X	X
Opprett rapport i alle formater	✓	✓	✓	✓
Rediger parametere for flaggingskriterier	✓	✓	✓	X
Parameterendring for automatisk fjerning av avvik	✓	✓	X	X
Aktiver automatisk fjerning av avvik	✓	✓	✓	X
Oppdater behandlingsmetode via FF/LS	✓	✓	X	X
Oppdater resultater via FF/LS	✓	✓	X	X
Aktiver gruppering etter addukt-funksjonalitet	✓	✓	X	X
Bla etter filer	✓	✓	✓	✓
Aktiver standardtilføyelsene	✓	✓	✓	X
Angi prosentregel	✓	X	X	X

Tabell 4-5: Forhåndsinnstilte tillatelser (fortsett)

Tillatelse	Administrator (Administrator)	Metodeutvikler	Analyst	Reviewer (Den som utfører gjennomgang)
for manuell integrering				
Vekt/volum	✓	✓	✓	X
Overskriv en resultattabell	✓	✓	✓	X
Merk resultatfilen som godkjent og lagre	✓	X	X	✓
Utforsker				
Tilgang til arbeidsområde for UTForsker	✓	✓	✓	✓
Export (Eksporter)	✓	✓	✓	X
Print (Skriv ut)	✓	✓	✓	X
Options (Alternativer)	✓	✓	✓	X
Kalibrer på nytt	✓	✓	X	X
Bla etter filer	✓	✓	✓	✓

Administrer brukere

Legge til en bruker eller gruppe

1. Åpne Configuration-arbeidsområdet.
2. Åpne User Management-siden.
3. Åpne Users-fanen.
4. Klikk på **Legg til bruker** ().
Dialogboksen Select User or Group åpnes.
5. Skriv inn navnet på en bruker eller gruppe, og klikk deretter på **OK**.

Tips! For informasjon om Select User or Group-dialogboksen og hvordan du bruker den, trykk på **F1**.

6. For å gjøre brukeren aktiv, sørg for at avmerkingsboksen **Aktiv bruker eller gruppe** er valgt.
7. Velg én eller flere roller i **Roles (Roller)**-området, og klikk deretter på **Save (Lagre)**.

Deaktiver brukere eller grupper

1. Åpne Configuration-arbeidsområdet.
2. Åpne User Management-siden.
3. Åpne Users-fanen.
4. Velg brukeren eller gruppen som skal deaktiveres i **Brukernavn eller -gruppe**-listen.
5. Tøm avmerkingsboksen **Aktiv bruker eller gruppe**.
Programvaren ber om bekreftelse.
6. Klikk på **Ja**.

Fjern brukere eller grupper

Bruk denne prosedyren for å fjerne en bruker eller gruppe fra programvaren. Hvis en bruker eller gruppe fjernes fra Windows, må brukeren også fjernes fra SCIEX OS-programvaren.

1. Åpne Configuration-arbeidsområdet.
2. Åpne User Management-siden.
3. Åpne Users-fanen.
4. Velg brukeren eller gruppen som skal fjernes i **Brukernavn eller -gruppe**-listen.
5. Klikk på **Delete (Slett)**.
Programvaren ber om bekreftelse.
6. Klikk på **OK**.

Administrer roller

Endre rollene som er tildelt en bruker eller gruppe

Bruk denne prosedyren for å tilordne nye roller til en bruker eller gruppe, eller for å fjerne eksisterende rolletildelinger.

1. Åpne Configuration-arbeidsområdet.
2. Åpne User Management-siden.
3. Åpne Users-fanen.
4. Velg brukeren eller gruppen som skal endres, i **Brukernavn eller -gruppe**-feltet.

5. Velg rollene som skal tilordnes til brukeren eller gruppen, og fjern eventuelle roller som skal fjernes.
6. Klikk på **Save (Lagre)**.

Lag en egendefinert rolle

1. Åpne Configuration-arbeidsområdet.
2. Åpne User Management-siden.
3. Åpne Roles-fanen.
4. Klikk på **Legg til rolle** ().
Dialogboksen Duplicate a User Role åpnes.
5. I **Eksisterende brukerrolle**-feltet velger du rollen som skal brukes som mal for den nye rollen.
6. Skriv inn et navn og en beskrivelse for rollen, og klikk deretter på **OK**.
7. Velg tilgangsprivilegier for rollen.
8. Klikk på **Lagre alle roller**.
9. Klikk på **OK**.

Slette en tilpasset rolle

Merk: Hvis en bruker bare er tildelt rollen som slettes, ber systemet om sletting av brukeren og rollen.

1. Åpne Configuration-arbeidsområdet.
2. Åpne User Management-siden.
3. Åpne Roles-fanen.
4. Klikk på **Slett en rolle**.
Dialogboksen Delete a User Role åpnes.
5. Velg rollen som skal slettes, og klikk deretter på **OK**.

Eksporter og importer brukeradministrasjonsinnstillinger

Brukeradministrasjonsdatabasen for SCIEX OS-programvaren kan eksporteres og importeres. Når du har konfigurert databasen for brukeradministrasjon på én SCIEX-datamaskin, kan du for eksempel eksportere den og deretter importere den til andre SCIEX-datamaskiner for å sikre at brukeradministrasjonsinnstillingene er konsistente.

Bare domenebrukere eksporteres. Lokale brukere eksporteres ikke.

Før du importerer brukeradministrasjonsinnstillinger, sikkerhetskopierer programvaren automatisk de gjeldende innstillingene. Du kan gjenopprette den siste sikkerhetskopien.

Eksporter innstillinger for brukeradministrasjon

1. Åpne Configuration-arbeidsområdet.
2. Åpne User Management-siden.
3. Klikk på **Advanced (Avansert) > Eksporter brukeradministrasjonsinnstillinger**. Dialogboksen Export User Management Settings åpnes.
4. Klikk på **Browse (Bla gjennom)**.
5. Bla til og velg mappen der innstillingene skal lagres, og klikk deretter på **Velg mappe**.
6. Klikk på **Export (Eksporter)**.
En bekreftelsesmelding vises med navnet på filen som inneholder de eksporterte innstillingene.
7. Klikk på **OK**.

Importer brukeradministrasjonsinnstillinger

Merk: Regulerde kunder: Hvis brukeradministrasjonsinnstillingene importeres etter programvarevalidering, anbefaler vi at den interne endringskontrollprosessen til å dokumentere konfigurasjonsendringene.

1. Åpne Configuration-arbeidsområdet.
2. Åpne User Management-siden.
3. Klikk på **Advanced (Avansert) > Importer brukeradministrasjonsinnstillinger**. Dialogboksen Import User Management Settings åpnes.
4. Klikk på **Browse (Bla gjennom)**.
5. Bla til og velg filen som inneholder innstillingene som skal importeres, og klikk deretter på **Open (Åpne)**.
Programvaren verifiserer at filen er gyldig.
6. Klikk på **Import (Importer)**.
Programvaren sikkerhetskopierer gjeldende brukeradministrasjonsinnstillinger og importerer de nye innstillingene. En bekreftelsesmelding vises.
7. Klikk på **OK**.

Gjenopprett brukeradministrasjonsinnstillinger

Før brukeradministrasjonsinnstillingene importeres, sikkerhetskopierer programvaren de gjeldende innstillingene. Bruk denne prosedyren for å gjenopprette den siste sikkerhetskopien av brukeradministrasjonsinnstillingene.

1. Åpne Configuration-arbeidsområdet.

2. Åpne User Management-siden.
3. Klikk på **Advanced (Avansert)** > **Gjenopprett tidligere innstillinger**. Dialogboksen Restore User Management Settings åpnes.
4. Klikk på **Ja**.
5. Lukk SCIEX OS-programvaren og åpne den på nytt.

Konfigurere tilgang til prosjekter og prosjektfiler

Bruk Windows-sikkerhetsfunksjonene til å kontrollere tilgangen til SCIEX OS Data-mappen. Prosjektfiler lagres som standard i SCIEX OS Data-mappen. For å få tilgang til et prosjekt må brukerne ha tilgang til rotkatalogen der prosjektdataene er lagret. For mer informasjon, se avsnittet: [Konfigurere Windows-sikkerhet](#).

Prosjektmapper

Hvert prosjekt inneholder mapper som lagrer forskjellige typer filer. Se tabellen for informasjon om innholdet i de forskjellige mappene: [Tabell 4-6](#).

Tabell 4-6: Prosjektmapper

Mappe	Innhold
\Acquisition Methods	Inneholder metodene for massespektrometer (MS) og LC som er opprettet i prosjektet. MS-metoder har msm-utvidelsen, og LC-metoder har lcm-utvidelsen.
\Audit Data	Inneholder prosjektrevisjonskartet og alle revisjonspostene.
\Batch	Inneholder alle innsamlingsbatchfilene som har blitt lagret. Innsamlingspartier har utvidelsen bch.
\Data	Inneholder innsamlingsdatafiler. Innsamlingsdatafiler har utvidelsene wiff og wiff2.
\Project Information	Inneholder prosjektets standardinnstillingsfiler.
\Quantitation Methods	Inneholder alle filene for behandlingsmetoden. Behandlingsmetoder har utvidelsen qmf.
\Quantitation Results	Inneholder alle tabellfilene for kvantifiseringsresultat. Resultattabellfiler har utvidelsen qsession.

Programvare-filtyper

For vanlige filtyper i SCIEX OS-programvaren, se tabellen: [Tabell 4-7](#).

Tabell 4-7: SCIEX OS-filer

Utvidelse	Filtype	Mappe
atds	- Revisjonssporingsdata og arkiver for arbeidsstasjoner - Innstillinger for revisjonssporinnstillinger for arbeidsstasjon - Data og arkiver for prosjektrevisjonsspor - Innstillinger for prosjektrevisjonsspor	- For prosjekter: <code><prosjektnavn>\Audit Data</code> - For arbeidsstasjonen: <code>C:\ProgramData\SCIEX\Audit Data</code>
atms	Revisjonskart	- For prosjekter: <code><prosjektnavn>\Audit Data</code> - For arbeidsstasjonen: <code>C:\ProgramData\SCIEX\Audit Data</code>
bch	Batch	Batch
cset	Resultattabell-innstillinger	Project Information
dat	Massespektrometri-datafil	Optimization
exml	Prosjektets standardinnstillinger	Prosjektinformasjon
journal	Midlertidige filer opprettet av SCIEX OS-programvaren	Forskjellige mapper
l cm	Metode	Innsamlingsmetoder
msm	MS metode	Innsamlingsmetoder
.pdf	Bærbare dokumentdata	—
qlayout	Arbeidsområdeoppsett	— Merk: Standard arbeidsområdeoppsett for et prosjekt lagres i Project Information (Prosjektinformasjon)-mappen.
qmethod	Behandlingsmetode	Kvantifiseringsmetoder
qsession	Results Table	Quantitation Results

Tabell 4-7: SCIEX OS-filer (fortsatt)

Utvidelse	Filtype	Mappe
	Merk: SCIEX OS-programvaren kan bare åpne qsession-filer som ble opprettet med SCIEX OS-programvaren.	
wiff	Massespektrometri-datafil som er kompatibel med SCIEX OS-programvaren Merk: SCIEX OS-programvaren lager både WIFF- og WIFF2-filer.	Data
wiff.scan	Massespektrometri-datafil	• Optimization • Data
wiff2	Massespektrometri-datafil generert av SCIEX OS-programvaren	• Optimal • Data
xls eller xlsx	Excel regneark	Batch (Parti)
xps	Rekalibrering	Data\Cal

Central Administrator Console (CAC)-programvaren er et valgfritt alternativ til lokal administrasjon med SCIEX OS-programvaren. CAC-programvaren inneholder administrasjon og tilpasning for sentral rolle, bruker, arbeidsstasjon og arbeidsgruppe, alt i ett program.

Denne delen beskriver CAC-programvaren og forklarer hvordan du konfigurerer og bruker den til å administrere personer, prosjekter og arbeidsstasjoner sentralt.

Merk: For å bruke CAC-programvaren og registrere arbeidsstasjoner med serveren, må du sørge for at SCIEX OS-programvaren er installert på hver arbeidsstasjon.

CAC-programvaren er lisensaktivert og kan installeres på alle arbeidsstasjoner som støtter SCIEX OS versjon 3.0 og Windows Server 2019.

CAC-programvaren er en del av SCIEX OS installasjonspakken. CAC-programvaren og SCIEX OS-programvaren kan imidlertid ikke installeres på samme datamaskin.

Bruker

Bruk User Management-siden til å legge til Windows-brukere og -grupper i databasen for brukeradministrasjon for SCIEX OS-programvaren. Administratoren kan også legge til, endre og slette brukerroller i delen User Roles and Permissions. For å få tilgang til programvaren må brukerne defineres i databasen for brukeradministrasjon, eller de må være medlem av en gruppe som er definert i databasen.

Brukerutvalg

Bare autoriserte brukere kan logge på arbeidsstasjonen og få tilgang til SCIEX OS-programvaren når SCIEX OS-programvaren administreres med Central Administrator Console (CAC)-programvaren. Før brukere kan legges til i arbeidsgrupper, må de legges til i brukerutvalget.

Legg til en bruker eller gruppe i brukerutvalget

1. Åpne Central Administration-arbeidsområdet.
2. Åpne User Management-siden.
3. Åpne User Pool-fanen.
4. Klikk på **Legg til brukere i brukerutvalget** ().
- Dialogboksen Select Users or Groups åpnes.
5. Skriv inn navnet på en bruker eller gruppe, og klikk deretter på **OK**.

Tips! Trykk på og hold nede **Ctrl**-tasten, og klikk deretter på **OK** for å velge flere brukere eller grupper.

Slett brukere eller grupper

1. Åpne Central Administration-arbeidsområdet.
2. Åpne User Management-siden.
3. Åpne User Pool-fanen.
4. Velg brukeren eller gruppen som skal slettes, og klikk deretter på **Delete (Slett)** i høyre rute.
Programvaren ber om bekreftelse.
5. Klikk på **OK**.

Brukerroller og tillatelser

Dette avsnittet beskriver User Roles and Permissions-siden.

Brukere kan tilordnes én eller flere av de forhåndsdefinerte rollene, beskrevet i følgende tabell, eller til egendefinerte roller, om nødvendig. Funksjonene som brukeren har tilgang til, er spesifisert av roller. De forhåndsdefinerte rollene kan ikke slettes, og deres tillatelser kan ikke endres.

Merk: I CAC-programvaren Central Administrator Console (CAC) kan brukerne også se den tidligste versjonen av SCIEX OS-programvaren som støtter tillatelser.

Tabell 5-1: Forhåndsinnstilte roller

Role (Rolle)	Typiske oppgaver
Administrator (Administrator)	• Administrerer systemet • Konfigurerer sikkerhet
Metodeutvikler	• Oppretter metoder • Kjører batcher • Analyserer data for bruk av brukeren
Analyst	• Kjører batcher • Analyserer data for bruk av brukeren
Reviewer (Den som utfører gjennomgang)	• Går gjennom data • Går gjennom revisjonsspor • Går gjennom kvantifiseringsresultater

Tabell 5-2: Forhåndsinnstilte tillatelser

Tillatelse	Administrator (Administrator)	Metodeutvikler	Analyst	Reviewer (Den som utfører gjennomgang)
Batch (Parti)				
Send inn ulåste metoder	✓	✓	✓	X
Open (Åpne)	✓	✓	✓	✓
Save As (Lagre som)	✓	✓	✓	X
Submit (Send inn)	✓	✓	✓	X
Save (Lagre)	✓	✓	✓	X
Lagre ionereferansetabell	✓	✓	✓	X
Legg til undermapper for data	✓	✓	✓	X
Konfigurer beslutningsregler	✓	✓	✓	X
Konfigurasjon				
Generell fane	✓	✓	X	X
Generelt: endre regional innstilling	✓	✓	X	X
Generelt: fullskjermmodus	✓	✓	X	X
LIMS kommunikasjons fane	✓	✓	X	X
Generelt: Stopp Windows-tjenester	✓	X	X	X
Fane for revisjonskart	✓	X	X	X
Kø-fane	✓	✓	✓	✓

Tabell 5-2: Forhåndsinnstilte tillatelser (fortsett)

Tillatelse	Administrator (Administrator)	Metodeutvikler	Analyst	Reviewer (Den som utfører gjennomgang)
Kø: instrumentets inaktive tid	✓	✓	X	X
Kø: maks. antall innsamlede prøver	✓	✓	X	X
Kø: andre køinnstillinger	✓	✓	X	X
Prosjekter-fane	✓	✓	✓	✓
Prosjekter: opprett prosjekt	✓	✓	✓	X
Prosjekter: bruk en revisjonskartmal på et eksisterende prosjekt	✓	X	X	X
Prosjekter: opprett rotkatalog	✓	X	X	X
Prosjekter: angi gjeldende rotkatalog	✓	X	X	X
Prosjekter: spesifiser nettverkslegitima sjon	✓	X	X	X
Prosjekter: Aktiver kontrollsumskriv ing for oppretting av wiff-data	✓	X	X	X
Prosjekter: tøm rotkatalog	✓	X	X	X
Enhetsfane	✓	✓	✓	X

Tabell 5-2: Forhåndsinnstilte tillatelser (fortsett)

Tillatelse	Administrator (Administrator)	Metodeutvikler	Analyst	Reviewer (Den som utfører gjennomgang)
Brukeradministrasjon-fane	✓	X	X	X
Tving avlogging av bruker	✓	X	X	X
CAC-fane ¹	✓	X	X	X
Fanen utskriftsmal:	✓	✓	X	X
Utskriftsmaler: Opprett og endre utskriftsmaler	✓	✓	X	X
Utskriftsmaler: Angi standard utskriftsmal	✓	✓	X	X
Utskriftsmaler: Bruk gjeldende mal på alle prosjekter i rotkatalogen	✓	X	X	X
Hendelseslogg				
Tilgang til arbeidsområdet for hendelseslogg	✓	✓	✓	✓
Arkivlogg	✓	✓	✓	✓
Revisjonsspor				
Tilgang til arbeidsområdet for revisjonsspor	✓	✓	✓	✓
Vis aktivt revisjonskart	✓	✓	✓	✓
Skriv ut/eksporter revisjonsspor	✓	✓	✓	✓

¹ I versjon 3.1 ble tillatelsen **Aktiver sentraladministrasjon** omdøpt til **CAC**. CAC-siden i Configuration-arbeidsområdet kan brukes til å konfigurere sentral administrasjon av SCIEX OS-programvaren.

Tabell 5-2: Forhåndsinnstilte tillatelser (fortsett)

Tillatelse	Administrator (Administrator)	Metodeutvikler	Analyst	Reviewer (Den som utfører gjennomgang)
Datainnsamlingspanel				
Start	✓	✓	✓	X
Stopp	✓	✓	✓	X
Save (Lagre)	✓	✓	✓	X
MS & LC-metode				
Tilgangsmetode for arbeidsområde	✓	✓	✓	✓
Nytt	✓	✓	X	X
Open (Åpne)	✓	✓	✓	✓
Save (Lagre)	✓	✓	X	X
Save As (Lagre som)	✓	✓	X	X
Låse-/ opplåsningsmetode	✓	✓	X	X
Kø				
Administrer	✓	✓	✓	X
Start/Stopp	✓	✓	✓	X
Print (Skriv ut)	✓	✓	✓	✓
Rediger prøve	✓	✓	X	X
Bibliotek				
Tilgang til bibliotekets arbeidsområde	✓	✓	✓	✓
MS tune				
Tilgang til MS Tune- arbeidsområdet	✓	✓	✓	X
Avansert MS- tuning	✓	✓	X	X

Tabell 5-2: Forhåndsinnstilte tillatelser (fortsett)

Tillatelse	Administrator (Administrator)	Metodeutvikler	Analyst	Reviewer (Den som utfører gjennomgang)
Avansert feilsøking	✓	✓	X	X
Hurtig statuskontroll	✓	✓	✓	X
Gjenoppsett instrumentdata	✓	✓	X	X
Analyse				
Nye resultater	✓	✓	✓	X
Opprett behandlingsmetoder	✓	✓	✓	X
Endre behandlingsmetode	✓	✓	X	X
Allow Export and Create Report of unlocked Results Table (Tillat eksport og opprett rapport om ulåste resultattabeller)	✓	X	X	X
Lagre resultater for automatiseringsbatch	✓	✓	✓	X
Change default quantitation method integration algorithm (Endre standardalgoritme for integrering av) kvantifiseringsmetoder	✓	✓	X	X
Change default quantitation	✓	✓	X	X

Tabell 5-2: Forhåndsinnstilte tillatelser (fortsatt)

Tillatelse	Administrator (Administrator)	Metodeutvikler	Analyst	Reviewer (Den som utfører gjennomgang)
method integration parameters (Endre standardparamet re for integrering av kvantifiseringsm etoder)				
Aktiver prosjektmodifise rt toppadvarsel	✓	X	X	X
Legg til prøver	✓	✓	✓	X
Fjern valgte prøver	✓	✓	✓	X
Eksporter, importer eller fjern ekstern kalibrering	✓	✓	✓	X
Endre prøvenavn	✓	✓	✓	X
Endre prøvetype	✓	✓	✓	X
Endre prøve-ID	✓	✓	✓	X
Endre faktisk konsentrasjon	✓	✓	✓	X
Endre fortynningsfakto r	✓	✓	✓	X
Endre kommentarfelt	✓	✓	✓	X
Aktiver manuell integrering	✓	✓	✓	X
Sett topp til 'Ikke funnet'	✓	✓	✓	X
Inkluder eller ekskluder en	✓	✓	✓	X

Tabell 5-2: Forhåndsinnstilte tillatelser (fortsett)

Tillatelse	Administrator (Administrator)	Metodeutvikler	Analyst	Reviewer (Den som utfører gjennomgang)
topp fra resultattabellen				
Regresjonsalternativer	✓	✓	✓	X
Endre integreringsparametre for resultattabell for et enkelt kromatogram	✓	✓	✓	X
Endre kvantifiseringsmetode for resultattabell-komponenten	✓	✓	✓	X
Opprett nye innstillinger for metrisk diagram	✓	✓	✓	✓
Legg til egendefinerte kolonner	✓	✓	✓	X
Angi tittelformat for gjennomgang av topper	✓	X	X	X
Remove custom column (Fjern egendefinert kolonne)	✓	✓	X	X
Visningsinnstillinger for resultattabell	✓	✓	✓	✓
Lås resultattabell	✓	✓	✓	✓
Lås opp resultattabell	✓	X	X	X
Merk resultatfilen som	✓	X	X	✓

Tabell 5-2: Forhåndsinnstilte tillatelser (fortsett)

Tillatelse	Administrator (Administrator)	Metodeutvikler	Analyst	Reviewer (Den som utfører gjennomgang)
gjennomgått og lagre				
Endre rapportmal	✓	✓	X	X
Overfør resultater til LIMS	✓	✓	✓	X
Endre strekkodekolonne	✓	✓	X	X
Endre sammenligningsprøvetildeling	✓	✓	X	X
Legg til MSMS-spektra i biblioteket	✓	✓	X	X
Prosjektets standardinnstillinger	✓	✓	X	X
Opprett rapport i alle formater	✓	✓	✓	✓
Rediger parametere for flaggingskriterier	✓	✓	✓	X
Parameterendring for automatisk fjerning av avvik	✓	✓	X	X
Aktiver automatisk fjerning av avvik	✓	✓	✓	X
Oppdater behandlingsmetode via FF/LS	✓	✓	X	X
Oppdater resultater via FF/LS	✓	✓	X	X

Tabell 5-2: Forhåndsinnstilte tillatelser (fortsett)

Tillatelse	Administrator (Administrator)	Metodeutvikler	Analyst	Reviewer (Den som utfører gjennomgang)
Aktiver gruppering etter addukt-funksjonalitet	✓	✓	X	X
Bla etter filer	✓	✓	✓	✓
Aktiver standardtilføyelse	✓	✓	✓	X
Angi prosentregel for manuell integrering	✓	X	X	X
Vekt/volum	✓	✓	✓	X
Utforsker				
Tilgang til arbeidsområde for UTForsker	✓	✓	✓	✓
Export (Eksporter)	✓	✓	✓	X
Print (Skriv ut)	✓	✓	✓	X
Options (Alternativer)	✓	✓	✓	X
Kalibrer på nytt	✓	✓	X	X

Legge til en tilpasset rolle

Central Administrator Console (CAC)-programvaren har fire forhåndsdefinerte roller. Hvis flere roller er påkrevd, kopierer du en eksisterende rolle og tildeler tilgangsrettigheter.

1. Åpne Central Administration-arbeidsområdet.
2. Åpne User Management-siden.
3. Åpne User Roles and Permissions-fanen.

4. Klikk på **Legg til rolle** ().
Dialogboksen Duplicate a User Role åpnes.

5. I **Eksisterende brukerrolle**-feltet velger du rollen som skal brukes som mal for den nye rollen.
6. Skriv inn et navn og en beskrivelse for rollen, og klikk deretter på **OK**. Den nye rollen vises i User Roles and Permission Categories-vinduet.
7. Velg tilgangsprivilegiene for rollen ved å merke av i de tilsvarende avmerkingsboksene.
8. Klikk på **Lagre alle roller**.

Slette en tilpasset rolle

1. Åpne Central Administration-arbeidsområdet.
2. Åpne User Management-siden.
3. Åpne User Roles and Permissions-fanen.
4. Klikk på **Slett en rolle**. Dialogboksen Delete a User Role åpnes.
5. Velg rollen som skal slettes, og klikk deretter på **OK**.

Arbeidsgrupper

Bruk Workgroup Management-siden til å administrere arbeidsgrupper. Arbeidsgrupper har brukere, arbeidsstasjoner og prosjekter.

Opprett en arbeidsgruppe ved å legge til ressurser fra de respektive gruppene. Før du oppretter arbeidsgrupper, må du sørge for å legge til alle potensielle brukere i brukerutvalget, arbeidsstasjoner i arbeidsstasjonsutvalget og prosjektkataloger i prosjektutvalget.

Legg om nødvendig til flere roller. Velg eventuelt sikkerhetsmodus for hver arbeidsgruppe.

Sikkerhetsmodusinnstillingen for arbeidsgruppen går foran sikkerhetsmodusinnstillingen for arbeidsstasjonen hvis arbeidsstasjonen er registrert med Central Administrator Console (CAC)-programvaren, og hvis den er medlem av arbeidsgruppen.

Ikke legg til lokale brukere i arbeidsgrupper. CAC-programvaren er et nettverksprogram, og bare nettverksbrukere skal legges til i en arbeidsgruppe.

Merk: I hver arbeidsgruppe må minst én bruker tilordnes administratorrolle. Bare en administrator eller arbeidsleder kan låse opp CAC-programvareskjermen hvis den påloggede brukeren er utilgjengelig.

Hvis serverbasert sikkerhet ikke lenger er nødvendig for en bestemt arbeidsstasjon, kan du administrere sikkerheten for arbeidsstasjonen lokalt med SCIEX OS-programvaren.

Opprette en arbeidsgruppe

1. Åpne Central Administration-arbeidsområdet.
2. Åpne Workgroup Management-siden.

3. Klikk på **Legg til arbeidsgruppe** ().
Dialogboksen Add a Workgroup åpnes.
4. Skriv inn et navn i feltet **Arbeidsgruppenavn**.
5. Skriv inn en beskrivelsen i **Beskrivelse**-feltet, og klikk deretter på **Add (Legg til)**.
Arbeidsgruppen opprettes og legges til i Manage Workgroups and Assignments-ruten. Central Administrator Console (CAC)-programvaren oppretter det aktuelle arbeidsgruppenavnet på serveren.

Merk: Integrert modus er standardsikkerhetsinnstillingen.

Slette en arbeidsgruppe

Hvis en arbeidsgruppe ikke lenger er nødvendig, må den slettes fra listen Arbeidsgruppe. Hvis du sletter en arbeidsgruppe, slettes bare arbeidsgruppen fra Central Administrator Console (CAC)-programvaren. Ingen data går tapt fra arbeidsstasjonen.

1. Åpne Central Administration-arbeidsområdet.
2. Åpne Workgroup Management-siden.
3. Utvid **Arbeidsgrupper**-listen, og finn arbeidsgruppen som skal slettes. Klikk på **Delete (Slett)**.
Dialogboksen Delete Workgroup åpnes.
4. Klikk på **Ja**.

Legg til brukere eller grupper i en arbeidsgruppe

Merk: Brukere som er lagt til i arbeidsgruppen, tildeles ikke automatisk en rolle. For å tildele roller til brukere, se avsnittet: [Legg til eller fjern en rolle](#).

1. Åpne Central Administration-arbeidsområdet.
2. Åpne Workgroup Management-siden.
3. I Manage Workgroups and Assignments-ruten utvider du arbeidsgruppen som skal endres, og deretter utvider du **Brukere**-listen.
4. Velg en bruker eller gruppe, og klikk deretter på **Add (Legg til)** ().

Tips! Legg til eller velg flere brukere ved å trykke på **Shift +** og deretter velge de nødvendige brukerne.

Brukeren eller gruppen legges til i gjeldende arbeidsgruppe.

5. Tilordne én eller flere roller til den tilordnede brukeren eller gruppen. Se avsnittet: [Legg til eller fjern en rolle](#).
6. Klikk på **Save (Lagre)**.

Legg til eller fjern en rolle

Forutsetninger for prosedyrer

- [Legg til brukere eller grupper i en arbeidsgruppe.](#)

For informasjon om å opprette roller i Central Administrator Console (CAC)-programvaren, se avsnittet: [Legg til en tilpasset rolle](#). Brukere eller grupper med en tildelt rolle har alle tillatelsene som er knyttet til rollen. Brukere eller grupper kan ha mer enn én rolle om gangen.

1. Åpne Central Administration-arbeidsområdet.
2. Åpne Workgroup Management-siden.
3. I Manage Workgroups and Assignments-ruten utvider du arbeidsgruppen som skal endres, og deretter utvider du **Brukere**-listen.
4. I Current Workgroup Membership-avsnittet tilordner eller fjerner du roller i **Tildel roller**-kolonnen.
5. Klikk på **Save (Lagre)**.

Legg til arbeidsstasjoner i en arbeidsgruppe

Merk: En arbeidsstasjon vises bare i arbeidsstasjonsutvalget hvis den er registrert med Central Administrator Console (CAC)-programvaren. Se avsnittet: [Legg til en arbeidsstasjon](#)

1. Åpne Central Administration-arbeidsområdet.
2. Åpne Workgroup Management-siden.
3. I Manage Workgroups and Assignments-ruten utvider du arbeidsgruppen som skal endres, og deretter utvider du **Arbeidsstasjoner**-listen.
4. Velg en arbeidsstasjon, og klikk deretter på **Add (Legg til)** ().
- Arbeidsstasjonen legges til den gjeldende arbeidsgruppen.
5. Klikk på **Save (Lagre)**.

Tilordne sikkerhetsinnstillinger for arbeidsstasjoner

Forutsetninger for prosedyrer

- [Legg til en arbeidsstasjon](#)
- [Legg til arbeidsstasjoner i en arbeidsgruppe](#)

For mer informasjon om sikkerhetsmoduser, se avsnittet: [Konfigurer sikkerhetsmodusen](#).

1. Åpne Central Administration-arbeidsområdet.
2. Åpne Workgroup Management-siden.

3. I Manage Workgroups and Assignments-ruten utvider du arbeidsgruppen som skal endres, og deretter utvider du **Arbeidsstasjoner**-listen.
4. (Valgfritt) For å gjøre gjeldende arbeidsgruppe til standardarbeidsgruppe for den arbeidsstasjonen merker du av i avkrysningsboksen **Sett som standard** i Current Workgroup Membership-avsnittet.
5. I Assign Security Settings-delen velger du **Security Mode (Sikkerhetsmodus)** for arbeidsgruppen, og deretter skriver du inn riktig **Skjermlås** og **Automatisk utlogging**-klokkeslett.
6. Klikk på **Save (Lagre)**.

Legg til prosjekter i en arbeidsgruppe

Merk: Denne prosedyren kreves bare hvis prosjekttilgang administreres sentralt.

Merk: Hvis et prosjekt legges til i mer enn én arbeidsgruppe, blir brukertilgang til prosjektet lagt til, ikke overskrevet. For eksempel har Arbeidsgruppe 1 Bruker A, Bruker B og Project_01. Arbeidsgruppe 2 har bruker B og bruker C. Hvis Project_01 legges til i arbeidsgruppe 2, vil bruker A, bruker B og bruker C alle ha tilgang til Project_01.

1. Åpne Central Administration-arbeidsområdet.
2. Åpne Workgroup Management-siden.
3. I Manage Workgroups and Assignments-ruten utvider du arbeidsgruppen som skal endres, og deretter utvider du **Projects (Prosjekter)**-listen.
4. Velg avmerkingsboksen **Bruk sentrale innstillinger for prosjekter**. Delen for prosjektvalg vises.
5. Velg en **Prosjektets rotkatalog** for å legge til en hel gruppe prosjekter, eller utvid prosjektroten og velg et bestemt prosjekt som skal legges til i arbeidsgruppen.
6. Klikk på **Add (Legg til)** () for å legge prosjektene til arbeidsgruppen. Prosjektroten legges til Current Workgroup Membership-tabellen. Utvid prosjektroten for å vise gjeldende prosjekter i arbeidsgruppen.
7. Klikk på **Save (Lagre)**.

Administrer prosjekter

Bruk Project Management-siden til å legge til, endre og slette prosjekter.

For å få tilgang til et prosjekt må brukerne ha tilgang til rotkatalogen der prosjektdataene er lagret. For mer informasjon, se avsnittet: [Om prosjekter og rotkataloger](#).

Om prosjekter og rotkataloger

En rotkatalog er en mappe som inneholder ett eller flere prosjekter. Det er mappen der programvaren ser etter prosjektdata. Den forhåndsdefinerte rotkatalogen er `D:\SCIEX OS Data`.

Opprett prosjekter ved hjelp av Central Administrator Console (CAC)-programvaren for å sikre at prosjektinformasjonen lagres på en sikker måte. Legg til prosjekter i Project Root Pool før du legger dem til i en arbeidsgruppe. Se avsnittet: [Legg til prosjekt](#).

Prosjektdata kan organiseres i undermapper. Opprett undermappene med CAC-programvaren. Se avsnittet: [Legg til en undermappe](#).

Merk: Hvis et prosjekt er opprettet utenfor CAC-programvaren, skal prosjektroten oppdateres etter at prosjektet er opprettet. Når roten oppdateres, synkroniseres innholdet av Project Root Pool med innholdet av prosjektrøttene på nettverket.

Legg til en rotkatalog

En rotkatalog er mappen der ett eller flere prosjekter er lagret.

Merk: Programvaren lagrer opptil ti rotkataloger.

Tips! Lokale stasjoner er ikke tilgjengelige på nettverket. En rotkatalog kan bare opprettes på en delt stasjon.

1. Åpne Central Administration-arbeidsområdet.
2. Åpne Project Management-siden.
3. Klikk på **Legg til ny eller eksisterende prosjektrot i prosjektutvalget** (). Dialogboksen Add Root Directory åpnes.
4. Skriv inn hele banen til rotkatalogmappen, og klikk deretter på **OK**. Mappen opprettes.

Tips! I stedet for å skrive inn banen, klikk på **Browse (Bla gjennom)**, og velg deretter mappen der rotkatalogen skal opprettes.

Tips! Du kan også opprette en mappe i File Explorer, og deretter bla til og velge mappen.

Merk: For installasjoner av SCIEX OS-programvaren med en behandlinglisens, kan rotkatalogen være en Analyst-programvare (`Analyst Data\Projects`).

5. Klikk på **OK**.
Den nye rotkatalogen blir rotkatalogen for det aktuelle prosjektet.

Slette en prosjektkatalog

Programvaren lagrer en liste over de siste ti rotkatalogene som ble brukt. Du kan slette rotkataloger fra denne listen.

Merk: Hvis du sletter en prosjektkatalog, slettes også alle tilknyttede prosjekter fra prosjekttutvalget.

1. Åpne Central Administration-arbeidsområdet.
2. Åpne Project Management-siden.
3. Finn prosjektets rotkatalog som skal slettes, og klikk deretter på **Slett prosjektrot** i Actions-delen.
Programvaren ber om bekreftelse.
4. Klikk på **OK**.

Legg til prosjekt

Forutsetninger for prosedyrer
• Legg til en rotkatalog

Prosjektet lagrer innhentingsmetoder, data, batcher, behandlingsmetoder, behandlingsresultater og så videre. Vi anbefaler bruk av en egen prosjektmappe for hvert prosjekt.

Ikke opprett prosjekter eller kopier eller lim inn filer utenfor Central Administrator Console (CAC)-programvaren.

1. Åpne Central Administration-arbeidsområdet.
2. Åpne Project Management-siden.
3. Klikk på **Legg til prosjekt** i Actions-delen av rotmappen.
Dialogboksen New Project åpnes.
4. Skriv inn prosjektnavnet.
5. Klikk på **OK**.
Det nye prosjektet vises under prosjektroten.

Legge til en undermappe

Data i prosjekter kan organiseres videre i undermapper.

1. Åpne Central Administration-arbeidsområdet.
2. Åpne Project Management-siden.
3. Klikk på **Legg til undermapper for data** i Actions-delen av rotmappen.
Dialogboksen Add Data Sub-Folders åpnes.

4. Velg et prosjekt som undermappen skal tilhøre.
5. Klikk på **Legg til en ny undermappe for data** ().
Dialogboksen Data Sub-Folder Name åpnes.
6. Skriv inn navnet på undermappen.
7. Klikk på **Save (Lagre)**.

Tips! Undermapper kan nestes i andre undermapper. For å opprette en nestet undermappe, velg en eksisterende undermappe i Project Data Sub-Folders-avsnittet,

og klikk deretter på **Legg til en ny undermappe for data** ().

8. Lukk Add Data Sub-Folders-dialogboksen.

Arbeidsstasjoner

Bruk Workstation Management-siden til å administrere alle arbeidsstasjonene som er koblet til CAC-programvaren. Arbeidsstasjoner som kontrolleres av CAC-programvaren, har automatisk tilpassede innstillinger.

Legg til en arbeidsstasjon

På Workstation Management-siden kan administratorer legge til arbeidsstasjoner, aktivere og deaktivere sentral kontroll av arbeidsstasjoner og fjerne arbeidsstasjoner.

1. Åpne Central Administration-arbeidsområdet.
2. Åpne Workstation Management-siden.
3. Klikk på **Legg til arbeidsstasjon i arbeidsstasjonsutvalget** ().
Dialogboksen Select Computers åpnes.
4. Skriv inn navnene på arbeidsstasjonene som skal legges til, og klikk deretter på **OK**.
Den sentrale administrasjonen **Status** av arbeidsstasjonen endres fra **Tilkobler** til **Disabled**.
5. (Valgfritt) For å aktivere sentral kontroll av arbeidsstasjonen:
 - a. I kolonnen **Status**, klikk på **Disabled**.
 - b. Klikk på **OK**.

Tips! Brukere kan også aktivere sentral administrasjon i SCIEX OS-programvaren. Se dokumentet: *SCIEX OS Hjelpesystem for programvare*.

Slette en arbeidsstasjon

Hvis en arbeidsstasjon ikke lenger er i bruk eller ikke lenger trenger å være en del av en arbeidsgruppe, sletter du arbeidsstasjonen fra arbeidsstasjonsutvalget. Hvis en arbeidsstasjon slettes, blir den fjernet fra hvilken som helst av arbeidsgruppene den ble tilordnet. Ingen data går tapt på arbeidsstasjonen når den fjernes.

1. Åpne Central Administration-arbeidsområdet.
2. Åpne Workstation Management-siden.
3. Klikk på **Arbeidsstasjonsadministrasjon**.
4. Finn arbeidsstasjonen som skal slettes i Workstation Pool-ruten, og klikk deretter på **Delete (Slett)**.
Dialogboksen Delete Workstation åpnes.
5. Klikk på **OK**.

Rapporter og sikkerhetsfunksjoner

Generere datarapporter

Bruk denne prosedyren for å generere datarapporter som inneholder detaljer som konfigurerte brukere, roller, arbeidsstasjoner, prosjekter og arbeidsgrupper.

1. Åpne Central Administration-arbeidsområdet.
2. Klikk på **Print (Skriv ut)**.
Dialogboksen Print Options åpnes.
3. Select the pages to print og klikk deretter på **Fortsett**.
4. Angi utskriftsalternativene, og klikk deretter på **Print (Skriv ut)**.
5. (Bare utskrift til PDF) Bla til stedet der rapporten skal lagres, og klikk deretter på **Save (Lagre)**.

Eksporter CAC for brukeradministrasjon

Bruk denne prosedyren for å eksportere sikkerhetsinnstillinger slik at de kan importeres til et annet Central Administrator Console (CAC)-system. Innstillingene eksporteres som en `ecac-fil`.

1. Åpne Central Administration-arbeidsområdet.
2. Klikk på **Advanced (Avansert) > Eksporter CAC-innstillinger**.
Dialogboksen Export CAC Settings åpnes.
3. Klikk på **Browse (Bla gjennom)**.
4. Bla til og velg mappen der innstillingene skal lagres, og klikk deretter på **Velg mappe**.
5. Klikk på **Export (Eksporter)**.

En bekreftelsesmelding vises med navnet på filen som inneholder de eksporterte innstillingene.

6. Klikk på **OK**.

Importer CAC for brukeradministrasjon

Forutsetninger for prosedyrer

- | |
|--|
| <ul style="list-style-type: none">• Eksporter CAC for brukeradministrasjon |
|--|

Bruk denne prosedyren for å importere sikkerhetsinnstillinger fra andre Central Administrator Console (CAC)-systemer. Innstillingene importeres fra en `ecac`-fil.

1. Åpne Central Administration-arbeidsområdet.
2. Åpne Configuration-arbeidsområdet.
3. Åpne User Management-siden.
4. Klikk på **Advanced (Avansert) > Importer CAC-innstillinger**. Dialogboksen Import CAC Settings åpnes.
5. Klikk på **Browse (Bla gjennom)**.
6. Bla til og velg filen som inneholder innstillingene som skal importeres, og klikk deretter på **Open (Åpne)**. Programvaren sørger for at filen er gyldig.
7. Klikk på **Import (Importer)**. Programvaren sikkerhetskopierer de gjeldende innstillingene og importerer deretter de nye innstillingene. En bekreftelsesmelding vises.

Merk: De importerte innstillingene brukes etter at programvaren har startet på nytt.

8. Klikk på **OK**.

Gjenopprett CAC-programvareinnstillinger

Bruk denne prosedyren for å importere de sist eksporterte `ecac`-innstillingene automatisk.

1. Åpne Central Administration-arbeidsområdet.
2. Klikk på **Advanced (Avansert) > Gjenopprett CAC-innstillinger**. Dialogboksen Restore CAC Settings åpnes.

Merk: De gjenopprettede innstillingene brukes etter at Central Administrator Console (CAC)-programvaren er startet på nytt.
--

3. Klikk på **Ja**.

Eksporter CAC brukeradministrasjonsinnstillinger

Bruk denne prosedyren for å eksportere brukeradministrasjonsinnstillinger som kan brukes på et annet Central Administrator Console (CAC)-system. Innstillingene eksporteres som en data-fil.

Merk: Eksporterte innstillinger kan bare importeres til et system med samme versjon av CAC-programvaren.

1. Åpne Configuration Management-arbeidsområdet.
2. Klikk på **Advanced (Avansert) > Eksporter brukeradministrasjonsinnstillinger**. Dialogboksen Export CAC Settings åpnes.
3. Klikk på **Browse (Bla gjennom)**.
4. Bla til og velg mappen der innstillingene skal lagres, og klikk deretter på **Velg mappe**.
5. Klikk på **Export (Eksporter)**.
En bekreftelsesmelding vises med navnet på filen som inneholder de eksporterte innstillingene.
6. Klikk på **OK**.

Importer CAC brukeradministrasjonsinnstillinger

Forutsetninger for prosedyrer
• Eksporter CAC brukeradministrasjonsinnstillinger

Bruk denne prosedyren for å importere sikkerhetsinnstillinger fra et annet Central Administrator Console (CAC)-system. Innstillingene importeres fra en datafil.

Merk: Eksporterte innstillinger kan bare importeres til et system med samme versjon av CAC-programvaren.

1. Åpne Configuration Management-arbeidsområdet.
2. Klikk på **Advanced (Avansert) > Importer brukeradministrasjonsinnstillinger**. Dialogboksen Import User Management Settings åpnes.
3. Klikk på **Browse (Bla gjennom)**.
4. Bla til og velg filen som inneholder innstillingene som skal importeres, og klikk deretter på **Open (Åpne)**.
Programvaren sørger for at filen er gyldig.
5. Klikk på **Import (Importer)**.
Programvaren sikkerhetskopierer de gjeldende innstillingene, og importerer deretter de nye innstillingene. En bekreftelsesmelding vises.

Merk: De importerte innstillingene brukes etter at CAC-programvaren har startet på nytt.

6. Klikk på **OK**.

Dette avsnittet beskriver hvordan nettverksinnsamling fungerer i SCIEX OS-programvaren og fordelene og begrensningene ved nettverksbaserte prosjekter. Den inneholder også prosedyrer for konfigurering av nettverksinnhenting.

Om nettverksinnsamling

Nettverksinnhenting kan brukes til å innhente data fra ett eller flere instrumenter til nettverksbaserte prosjektmapper som kan behandles på eksterne arbeidsstasjoner. Denne prosessen er nettverksfeiltolerant, og sørger for at ingen data går tapt hvis nettverkstilkoblingen mislykkes under innhenting.

Systemtelsen kan være langsommere når nettverksprosjekter brukes enn når lokale prosjekter brukes. Fordi noen revisjonsspor også finnes i nettverksmappene, er enhver aktivitet som genererer en prosjektrevisjonsoppføring også tregere. Nettverksfiler kan ta litt tid å åpne, avhengig av nettverksytelsen. Nettverksytelsen er ikke bare relatert til den fysiske nettverksmaskinvaren, men også til nettverkstrafikk og -design.

Merk: Hvis ClearCore2-tjenesten avbrytes under nettverksinnsamlingen, skrives ikke de delvise prøvedataene for prøven i innsamlingen på tidspunktet for avbruddet til datafilen.

Merk: Når man bruker nettverksinnhenting i et regulert miljø, må man synkronisere det lokale klokkeslettet med servertiden for å få nøyaktige tidsstempler. Servertiden brukes til filopprettingstiden. Audit Trail Manager registrerer filoprettelsestiden ved hjelp av den lokale datatiden.

OBS: Potensielt datatap. Ikke lagre data fra flere innsamlingsdatamaskiner i samme nettverksdatafil.

Fordelene ved å bruke nettverksinnsamling

Innhenting av nettverksdata er en sikker metode for å arbeide med prosjektmapper som ligger helt på nettverksservere. Dette reduserer kompleksiteten som er involvert i innsamling av data lokalt og deretter flytting av dataene til et nettverkssted for lagring. Fordi nettverksstasjoner vanligvis sikkerhetskopieres automatisk, reduseres eller elimineres også behovet for sikkerhetskopiering av lokale stasjoner.

Sikker nettverkskonto

Under nettverksinnsamling bruker SCIEX OS-programvaren legitimasjonen til den gjeldende eller sist påloggede brukeren til å overføre data til nettverksmappen. Hvis brukeren som

startet innhenting, logger av, og en bruker som ikke har den nødvendige tilgangen til nettverksmappen, logger på, stopper overføringen av eksempeldata til nettverket.

For å forhindre dette anbefaler vi bruk av en sikker nettverkskonto (SNA). Hvis en SNA er konfigurert, bruker programvaren legitimasjonen til SNA til å overføre prøvedata til nettverksmappen.

SNA trenger ikke:

- Tilhører administratorgruppen på datamaskinen.
- Vær i User Management (Brukeradministrasjon)-databasen for SCIEX OS-programvaren.

SNA er spesifisert på Projects (Prosjekter)-siden i Configuration (Konfigurasjon)-arbeidsområdet. Bare en gyldig Windows-nettverks- eller domenekonto kan angis.

Tabellen som følger viser tillatelsene som kreves for nettverksinnsamling, for systemkontoen, SNA-en og brukeren som oppretter metoder og sender inn batcher.

Merk: Brukere måtte også ha tilgang til den installerte rotkatalogen. Se avsnittet: [Windows-tillatelser](#).

Tabell 6-1: Tillatelser for nettverksinnhenting

Konto	Nettverksprosjektmappe	SCIEX OS Data \TempData
SYSTEM	I/A	Full control
SNA	• Traverse folder / execute file • List folder / read data • Read attributes • Read extended attributes • Create files / write data • Create folders / append data • Write attributes • Write extended attributes • Read permissions	Full control
Bruker (med SNA)	• Traverse folder / execute file • List folder / read data • Read attributes	Arvet fra den installerte rotkatalogen

Tabell 6-1: Tillatelser for nettverksinnhenting (fortsett)

Konto	Nettverksprosjektmappe	SCIEX OS Data \TempData
	• Read extended attributes • Create files / write data • Create folders / append data • Write attributes • Write extended attributes • Read permissions	
Bruker (uten SNA)	• Traverse folder / execute file • List folder / read data • Read attributes • Read extended attributes • Create files / write data • Create folders / append data • Write attributes • Write extended attributes • Read permissions	Full control

Dataoverføringsprosess

Når SCIEX OS-programvaren henter inn data til en nettverksplassering, skriver den først hvert eksempel til en mappe på den lokale stasjonen, og overfører det deretter til nettverket. Etter at programvaren har fått bekreftelse på at alle dataene for batchen er overført, sletter den lokale mappen som inneholder dataene når neste batch starter. Hvis nettverket blir utilgjengelig under overføringen av prøvedataene, prøver programvaren igjen hvert 15. minutt til overføringen er vellykket.

Merk: Hvis ClearCore2-tjenesten stoppes under nettverksinnsamlingen, skrives ikke de delvise prøvedataene for prøven i innsamlingen på tidspunktet for avbruddet til datafilen.

Merk: Hvis du vil se data i sanntid i Explorer-arbeidsområdet under innhenting til en nettverksressurs, kan du gjøre følgende:

- Åpne Data Acquisition-panelet nederst i SCIEX OS-vinduet.
- I Queue-arbeidsområdet dobbeltklikker du på prøven som er under innhenting.

Hvis en prøve er åpen i Explorer-arbeidsområdet, vises følgende melding etter at prøven er flyttet til nettverksressursen: `File not found message`.

Konfigurer nettverksinnsamling

En rotkatalog er mappen der SCIEX OS-programvaren lagrer data. Opprett rotkatalogen med SCIEX OS-programvaren for å være sikker på at prosjektinformasjonen lagres på en sikker måte. Ikke opprett prosjekter i File Explorer.

Når du oppretter rotkataloger på en nettverksressurs, kan du eventuelt definere **Legitimasjon for sikker nettverkskonto**. Dette er den sikre nettverkskontoen som er definert på nettverksressursen. Se avsnittet: [Sikker nettverkskonto](#).

For informasjon om å opprette prosjekter og underprosjekter, se dokumentet: *SCIEX OS Brukerveiledning for programvare*.

For informasjon om å opprette prosjekter og underprosjekter, se dokumentet: *Topaz systembrukerveiledning*.

Spesifiser en sikker nettverkskonto

Hvis prosjekter lagres på en nettverksressurs, kan en SNA angis for å sikre at alle brukere av arbeidsstasjonen har den nødvendige tilgangen til nettverksressursen.

1. Åpne Configuration-arbeidsområdet.
2. Klikk på **Projects (Prosjekter)**.
3. I avsnittet **Advanced (Avansert)** klikker du på **Legitimasjon for sikker nettverkskonto**.
4. Skriv inn brukernavn, passord og domene for den sikre nettverkskontoen som er definert på nettverksressursen.
5. Klikk på **OK**.

Dette avsnittet forklarer hvordan du bruker revisjonsfunksjonen. For informasjon om Windows revisjonsfunksjoner, se avsnittet: [Systemrevisjoner](#).

Revisjonsspor

Programvaren organiserer revisjonshendelser i Audit Trail-arbeidsområdet. Programvaren lagrer hendelsene i revisjonsspor, som er filer som lagrer oppføringer over reviderte hendelser.

Hendelser i arbeidsstasjonen lagres i arbeidsstasjonens revisjonsspor. Revisjonsspor for arbeidsstasjoner er filer som lagrer de reviderte hendelsene for datamaskinen som SCIEX OS-programvaren er installert på.

CAC-systemhendelser er lagret i CAC-revisjonssporet.

Prosjektaktiviteter lagres i prosjektets revisjonsspor. Arbeidsområdet Audit Trail viser revisjonssporene for prosjektene i den aktive rotkatalogen. Behandling av hendelser i revisjonsspor finnes i prosjektets revisjonsspor og lagres med resultattabellen.

For en liste over reviderte hendelser, se avsnittet: [Revisjonshendelser](#).

Revisjonsspor, kombinert med filer som `wiff2`-filer og resultattabellfiler, utgjør gyldige elektroniske poster som kan brukes til samsvar.

Tabell 7-1: Revisjonsspor

Revisjonsspor	Eksempler på hendelser registrert	Tilgjengelige revisjonskart lagret i	Standard revisjonskart
Arbeidsstasjon (SCIEX OS)	• Endringer i: • Tildeling av aktivt revisjonskart • Instrumentinnstilling • Prøvekøer • Sikkerhet • Innstilling • Enheter	• C: \ProgramData \SCIEX\Audit Data-mappen	• Intet revisjonskart

Tabell 7-1: Revisjonsspor (fortsett)

Revisjonsspor	Eksempler på hendelser registrert	Tilgjengelige revisjonskart lagret i	Standard revisjonskart
CAC	• Endringer i: • Revisjonskart • CAC • Sikkerhet • Brukerlogg	• C:\ProgramData\SCIEX\Audit Data-mappen	• Stille revisjonskart
Prosjekt (ett per prosjekt)	• Endringer i: • Aktiv revisjonskarttildeling (SCIEX OS) • Prosjekt • Data • Utskrift	• <project>\Audit Data-mappe	• Spesifisert på Audit Maps-siden for Configuration-arbeidsområdet

Etter at et revisjonsspor inneholder 20,000 revisjonsopptak, vil SCIEX OS og CAC-programvaren automatisk arkivere opptakene og starte et nytt revisjonsspor. For mer informasjon, se avsnittet: [Revisjonssporarkiver](#).

Revisjonskart

Et revisjonskart er en fil som inneholder en liste over alle hendelsene som kan revideres, og om en grunn til endring eller elektronisk signatur er nødvendig for hendelsen. I SCIEX OS-programvaren finnes det to typer revisjonskart: arbeidsstasjon og prosjekt. I CAC er to typer revisjonskart tilgjengelige: CAC og prosjekt.

Revisjonskart for arbeidsstasjoner kontrollerer hendelsene som er revidert på en arbeidsstasjon.

Prosjektrevisjonskart styrer hendelsene som revideres for et prosjekt, og lagres i prosjektmappen.

Merk: Revisjonskartet for et prosjekt kan redigeres i enten SCIEX OS eller Central Administrator Console (CAC)-programvaren.

Brukeren kan opprette mange revisjonskart, men bare ett revisjonskart kan være i bruk om gangen for hver arbeidsstasjon, hvert CAC-system og hvert prosjekt. Revisjonskartet

Revisjon

som brukes for en arbeidsstasjon, et CAC-system eller et prosjekt,, kalles det aktive revisjonskartet.

Når SCIEX OS-programvaren er installert, er standard revisjonskart for alle nye prosjekter No Audit Map. Når CAC-programvaren er installert, er standard revisjonskart for alle nye prosjekter Silent Audit Map. Brukeren kan identifisere et annet aktivt revisjonskart som skal brukes som standard for alle nye prosjekter. Se avsnittet: [Endre det aktive revisjonskartet for et prosjekt](#).

Oppsett av revisjonskart

Før du arbeider med prosjekter som krever revisjon, må du konfigurere revisjonskart som gjelder for vanlige driftsprosedyrer. Flere standardmaler for revisjonskart er tilgjengelige når programvaren er installert, men det kan være nødvendig å opprette et tilpasset kart. Kontroller at ett revisjonskart er tilgjengelig for arbeidsstasjonen eller CAC-revisjonssporet og at ett revisjonskart er tilgjengelig for hvert prosjekt.

Tabell 7-2: Sjekkliste for konfigurering av revisjon

Oppgave	Se
• SCIEX OS: Lag et revisjonskart for revisjonssporet for arbeidsstasjon. • CAC-programvare: Lag et revisjonskart for CAC-revisjonssporet-revisjonssporet.	• SCIEX OS: • Opprett et revisjonskart for arbeidsstasjon • Redigere et revisjonskart for arbeidsstasjon • CAC-programvare: • Opprett et CAC-revisjonskart • Redigere et CAC-revisjonskart
• SCIEX OS: Bruk revisjonskartet til arbeidsstasjonens revisjonsspor. • CAC-programvare: Bruk revisjonskartet til CAC-revisjonssporet.	• SCIEX OS: Endre aktivt revisjonskart for en arbeidsstasjon • CAC programvare: Endre aktivt revisjonskart for et CAC-system
Opprett et standard aktivt revisjonskart for nye prosjekter.	• Opprett et prosjektrevisjonskart.
Konfigurer det revisjonskartet som skal brukes for hvert eksisterende prosjekt.	• Opprett et prosjektrevisjonskart. • Redigere et revisjonskart.
Bruk et revisjonskart til hvert eksisterende prosjekt.	• Endre det aktive revisjonskartet for et prosjekt.

Installerte revisjonskartmaler

Programvaren inkluderer flere revisjonskartmaler. Disse malene kan ikke redigeres eller slettes.

Tabell 7-3: Installerte revisjonskart

Revisjonskart	Beskrivelse
Eksempelrevisjonskart	Valgte hendelser blir revidert. Kun for illustrasjonsformål.
Full Audit Map (Fullt revisjonskart)	Alle hendelser blir revidert. Elektroniske signaturer og årsaker kreves for alle hendelsene.
No Audit Map (Intet revisjonskart)	Ingen hendelser blir revidert. Merk: Endre tildeling av aktivt revisjonskart -hendelsen registreres alltid, selv om malen No Audit Map brukes.
Silent Audit Map (Stille revisjonskart)	Alle hendelser blir revidert. Elektroniske signaturer og årsaker er ikke påkrevd for noen hendelser.

For beskrivelser av de tre typene revisjonsspor og deres forhold til revisjonskart, se tabellen: [Tabell 7-1](#). For informasjon om hendelsene som er registrert i revisjonsspor, se avsnittet: [Revisjonssporregistreringer](#).

For informasjon om revisjonsprosessen, se tabell: [Tabell 7-2](#).

Arbeid med revisjonskart

Programvaren inneholder flere installerte revisjonskartmaler. For beskrivelser av revisjonskartmalene, se avsnittet: [Installerte revisjonskartmaler](#). For en sjekkliste med foreslåtte trinn for å sette opp revisjon, se avsnittet: [Oppsett av revisjonskart](#).

Hvis en aktiv revisjonskartmal slettes i programvaren eller i File Explorer, bruker prosjektet som bruker denne revisjonskartmalen et stille revisjonskart.

Revisjonskart for prosjekt

Prosjektrevisjonskart styrer revisjonen av prosjekthendelser. For en liste over prosjekthendelser som kan revideres, se avsnittet: [Revisjonsspor for prosjekt](#).

Opprett et prosjektrevisjonskart

1. Åpne Configuration-arbeidsområdet.
2. Klikk på **Revisjonskart**.
3. Åpne Projects Templates-fanen.

Revisjon

4. I **Rediger kartmal**-feltet velger du en mal som skal brukes som grunnlag for det nye kartet.
5. Klikk på **Legg til mal** ().
Dialogboksen Add a Project Audit Map Template åpnes.
6. Skriv inn navnet på det nye kartet, og klikk deretter på **OK**.
7. Velg og konfigurert hendelsene som skal registreres ved å følge disse trinnene:
 - a. Velg **Revidert**-avmerkingsboksen er valgt for hendelsen.
 - b. (Valgfritt) Hvis det kreves en grunn, velger du **Årsak påkrevd**.
 - c. (Valgfritt) Hvis en elektronisk signatur kreves, velger du **E-sig påkrevd**.
 - d. (Valgfritt) Hvis det kreves forhåndsdefinerte årsaker, velger du **Bruk kun forhåndsdefinert årsak** og definerer årsakene.
8. Sørg for at **Revidert**-avmerkingsboksen er fjernet for alle aktiviteter som ikke skal revideres.
9. Klikk på **Lagre som mal**.
Systemet ber brukeren om å bruke det nye kartet på prosjekter.
10. Gjør ett av følgende:
 - Hvis du vil bruke det nye kartet på prosjekter, klikk på **Ja**, velg prosjektene som skal bruke det nye kartet, og klikk deretter på **Apply (Bruk)**.
 - Hvis det nye kartet ikke skal brukes på eksisterende prosjekter, klikker du på **Nei**.
11. (Valgfritt) Hvis du vil bruke dette revisjonskartet som standard for alle nye prosjekter, klikker du på **Bruk som standard for nye prosjekter**.

Redigere et revisjonskart

Merk: Installerte revisjonskartmaler kan ikke redigeres.

1. Åpne Configuration-arbeidsområdet.
2. Klikk på **Revisjonskart**.
3. Åpne Projects Templates-fanen.
4. I **Rediger kartmal**-feltet velger du kartet som skal endres.
5. Velg og konfigurert hendelsene som skal registreres ved å følge disse trinnene:
 - a. Velg **Revidert**-avmerkingsboksen for hendelsen.
 - b. (Valgfritt) Hvis det kreves en grunn, velger du **Årsak påkrevd**.
 - c. (Valgfritt) Hvis en elektronisk signatur kreves, velger du **E-sig påkrevd**.
 - d. (Valgfritt) Hvis det kreves forhåndsdefinerte årsaker, velger du **Bruk kun forhåndsdefinert årsak** og definerer årsakene.

6. Forsikre deg om at **Revidert**-avmerkingsboksen er tom for alle aktiviteter som ikke skal revideres.
7. Klikk på **Lagre som mal**.
Systemet ber brukeren om å bruke det nye kartet på prosjekter.
8. Gjør ett av følgende:
 - Hvis du vil bruke det nye kartet på prosjekter, klikk på **Ja**, velg prosjektene som skal bruke det nye kartet, og klikk deretter på **Apply (Bruk)**.
 - Hvis det nye kartet ikke skal brukes på eksisterende prosjekter, klikk på **Nei**.

Endre det aktive revisjonskartet for et prosjekt

Når et revisjonskart brukes i prosjektet, blir det det aktive revisjonskartet. Revisjonskonfigurasjonen i det aktive revisjonskartet bestemmer hvilke hendelser som blir registrert i revisjonssporene.

1. Åpne Configuration-arbeidsområdet.
2. Klikk på **Revisjonskart**.
3. Åpne Projects Templates-fanen.
4. I **Rediger kartmal**-feltet velger du revisjonskartet som skal tilordnes til prosjektet.
5. Klikk på **Bruk på eksisterende prosjekter**.
Dialogboksen Apply Project Audit Map Template åpnes.
6. Velg avmerkingsboksene for prosjektene som dette revisjonskartet skal gjelde for.
7. Klikk på **Apply (Bruk)**.

Slett et prosjektrevisjonskart

Merk: Installerte revisjonskartmaler kan ikke slettes.

1. Åpne Configuration-arbeidsområdet.
2. Klikk på **Revisjonskart**.
3. Åpne Projects Templates-fanen.
4. I **Rediger kartmal**-feltet velger du kartet som skal slettes.
5. Klikk på **Slett mal**.
Systemet ber om bekreftelse.
6. Klikk på **Ja**.

Revisjonskart for arbeidsstasjon

Revisjonskart for arbeidsstasjoner styrer revisjonen av arbeidsstasjonshendelser. For en liste over arbeidsstasjonshendelser som kan revideres, se avsnittet: [Revisjonsspor for arbeidsstasjon](#).

Opprett et revisjonskart for arbeidsstasjon

1. Åpne Configuration-arbeidsområdet.
2. Klikk på **Revisjonskart**.
3. Åpne Workstation Templates-fanen.
4. I **Rediger kartmal**-feltet velger du en mal som skal brukes som grunnlag for det nye kartet.
5. Klikk på **Legg til mal** ().
Dialogboksen Add a Workstation Audit Map Template åpnes.
6. Skriv inn navnet på det nye kartet, og klikk deretter på **OK**.
7. Velg og konfigurere hendelsene som skal registreres ved å følge disse trinnene:
 - a. Velg **Revidert**-avmerkingsboksen for hendelsen.
 - b. (Valgfritt) Hvis det kreves en grunn, velger du **Årsak påkrevd**.
 - c. (Valgfritt) Hvis en elektronisk signatur kreves, velger du **E-sig påkrevd**.
 - d. (Valgfritt) Hvis det kreves forhåndsdefinerte årsaker, velger du **Bruk kun forhåndsdefinert årsak** og definerer årsakene.
8. Forsikre deg om at **Revidert**-avmerkingsboksen er tom for alle aktiviteter som ikke skal revideres.
9. Klikk på **Lagre som mal**.
10. (Valgfritt) Hvis du vil bruke dette revisjonskartet som det aktive revisjonskartet for arbeidsstasjonen, klikker du på **Bruk på arbeidsstasjonen**.

Redigere et revisjonskart for arbeidsstasjon

Merk: Installerte revisjonskartmaler kan ikke redigeres.

1. Åpne Configuration-arbeidsområdet.
2. Klikk på **Revisjonskart**.
3. Åpne Workstation Templates-fanen.
4. I **Rediger kartmal**-feltet velger du kartet som skal endres.
5. Velg og konfigurere hendelsene som skal registreres ved å følge disse trinnene:
 - a. Velg **Revidert**-avmerkingsboksen for hendelsen.
 - b. (Valgfritt) Hvis det kreves en grunn, velger du **Årsak påkrevd**.
 - c. (Valgfritt) Hvis en elektronisk signatur kreves, velger du **E-sig påkrevd**.
 - d. (Valgfritt) Hvis det kreves forhåndsdefinerte årsaker, velger du **Bruk kun forhåndsdefinert årsak** og definerer årsakene.

6. Sørg for at avmerkingsboksen **Revidert** er fjernet for alle aktiviteter som ikke skal revideres.
7. Klikk på **Lagre som mal**.
8. (Valgfritt) For å bruke dette revisjonskartet som det aktive revisjonskartet for arbeidsstasjonen, klikker du på **Bruk på arbeidsstasjonen**.

Endre aktivt revisjonskart for en arbeidsstasjon

Når et revisjonskart brukes på arbeidsstasjonen, blir det det aktive revisjonskartet. Revisjonskonfigurasjonen i det aktive revisjonskartet bestemmer hvilke hendelser som blir registrert i revisjonssporene.

1. Åpne Configuration-arbeidsområdet.
2. Klikk på **Revisjonskart**.
3. Åpne Workstation Templates-fanen.
4. I **Rediger kartmal**-feltet velger du kartet som skal brukes på arbeidsstasjonen.
5. Klikk på **Bruk på arbeidsstasjonen**.

Slette et revisjonskart for arbeidsstasjon

Merk: Installerte revisjonskartmaler kan ikke slettes.

1. Åpne Configuration-arbeidsområdet.
2. Klikk på **Revisjonskart**.
3. Åpne Workstation Templates-fanen.
4. I **Rediger kartmal**-feltet velger du kartet som skal slettes.
5. Klikk på **Slett mal**.
Systemet ber om bekreftelse.
6. Klikk på **Ja**.

CAC Revisjonskart

CAC revisjonskart kontrollerer revisjon av CAC arbeidsstasjonshendelser. For en liste over revisjonshendelser, se avsnittet: [Revisjonsspor for arbeidsstasjon](#).

Opprett et CAC-revisjonskart

1. Åpne Configuration-arbeidsområdet.
2. Klikk på **Revisjonskart**.
3. Åpne CAC Templates-fanen.
4. I **Rediger kartmal**-feltet velger du en mal som skal brukes som grunnlag for det nye kartet.

5. Klikk på **Legg til mal** ().
Dialogboksen Add a CAC Audit Map Template åpnes.
6. Skriv inn navnet på det nye kartet, og klikk deretter på **OK**.
7. Velg og konfigurer hendelsene som skal registreres ved å følge disse trinnene:
 - a. Velg **Revidert**-avmerkingsboksen for hendelsen.
 - b. (Valgfritt) Hvis det kreves en grunn, velger du **Årsak påkrevd**.
 - c. (Valgfritt) Hvis en elektronisk signatur kreves, velger du **E-sig påkrevd**.
 - d. (Valgfritt) Hvis det kreves forhåndsdefinerte årsaker, velger du **Bruk kun forhåndsdefinert årsak** og definerer årsakene.
8. Forsikre deg om at **Revidert**-avmerkingsboksen er tom for alle aktiviteter som ikke skal revideres.
9. Klikk på **Lagre som mal**.
10. (Valgfritt) Hvis du vil bruke dette revisjonskartet som det aktive revisjonskartet for CAC-arbeidsstasjonen, klikker du på **Bruk på CAC**.

Redigere et CAC-revisjonskart

Merk: Installerte revisjonskartmaler kan ikke redigeres.

1. Åpne Configuration-arbeidsområdet.
2. Klikk på **Revisjonskart**.
3. Åpne CAC Templates-fanen.
4. I **Rediger kartmal**-feltet velger du kartet som skal endres.
5. Velg og konfigurer hendelsene som skal registreres ved å følge disse trinnene:
 - a. Velg **Revidert**-avmerkingsboksen for hendelsen.
 - b. (Valgfritt) Hvis det kreves en grunn, velger du **Årsak påkrevd**.
 - c. (Valgfritt) Hvis en elektronisk signatur kreves, velger du **E-sig påkrevd**.
 - d. (Valgfritt) Hvis det kreves forhåndsdefinerte årsaker, velger du **Bruk kun forhåndsdefinert årsak** og definerer årsakene.
6. Sørg for at avmerkingsboksen **Revidert** er fjernet for alle aktiviteter som ikke skal revideres.
7. Klikk på **Lagre som mal**.
8. (Valgfritt) Hvis du vil bruke dette revisjonskartet som det aktive revisjonskartet for CAC-arbeidsstasjonen, klikker du på **Bruk på CAC**.

Endre aktivt revisjonskart for et CAC-system

Når et revisjonskart brukes på CAC-arbeidsstasjonen, blir det det aktive revisjonskartet. Revisjonskonfigurasjonen i det aktive revisjonskartet bestemmer hvilke hendelser som blir registrert i revisjonssporene.

1. Åpne Configuration-arbeidsområdet.
2. Klikk på **Revisjonskart**.
3. Åpne CAC Templates-fanen.
4. I **Rediger kartmal**-feltet velger du kartet som skal brukes på CAC-arbeidsstasjonen.
5. Klikk på **Bruk på CAC**.

Slett et CAC-revisjonskart

Merk: Installerte revisjonskartmaler kan ikke slettes.

1. Åpne Configuration-arbeidsområdet.
2. Klikk på **Revisjonskart**.
3. Åpne CAC Templates-fanen.
4. I **Rediger kartmal**-feltet velger du kartet som skal slettes.
5. Klikk på **Slett mal**.
Systemet ber om bekreftelse.
6. Klikk på **Ja**.

Vise, søke, eksportere og skrive ut revisjonsspor

Denne delen gir informasjon om visning av revisjonsspor og arkiverte revisjonsspor. Det gir også instruksjoner for eksport, utskrift, søk og sortering av revisjonsjournaler i revisjonsspor.

Vise revisjonssporoppføringer

1. Åpne Audit Trail-arbeidsområdet.
2. I venstre rute klikker du på revisjonssporet som skal vises.
3. Klikk på aktiviteten for å se detaljert informasjon om en revisjonshendelse.
Den valgte aktivitetstypen styrer informasjonen som vises. Informasjonen vises på en eller flere av de følgende fanene.

Tabell 7-4: Faneer for hendelsesdetaljer

Fane	informasjon
General Details	Viser informasjon som tidssoneforskyvning, arbeidsstasjonsnavn og SCIEX OS programvareversjon.
Before Change	Viser innholdet før endringen ble gjort.
After Change	Viser innholdet etter at endringen ble gjort.
Change Details	Viser det opprinnelige innholdet og det nye innholdet i samme rute. I Difference View vises det opprinnelige innholdet i rødt og det nye innholdet i grønt. I Side By Side View vises det opprinnelige og det nye innholdet i separate ruter, slik at brukeren enkelt kan se endringene.
Print Details	Viser informasjonen som ble skrevet ut.

Søke etter eller filtrere en revisjonsoppføring

1. Åpne Audit Trail-arbeidsområdet.
2. Velg revisjonssporet som skal søkes i.
3. For å søke etter spesifikk overvåkingspost, skriv inn tekst i **Søk på side**-feltet. Alle forekomster av den angitte teksten på siden er uthøvet.
4. Følg disse trinnene for å filtrere revisjonssporoppføringerne:
 - a. Klikk på filterikonet (trakt). Dialogboksen Filter Audit Trail åpnes.
 - b. Skriv inn filterkriteriene.
 - c. Klikk på **OK**.

Vise et arkivert revisjonsspor

Etter at et revisjonsspor inneholder 20 000 revisjonsjournaler, arkiverer SCIEX OS-programvaren automatisk journalene og begynner et nytt revisjonsspor. De arkiverte revisjonssporfilene er navngitt med type revisjonsspor og dato og klokkeslett. For eksempel har filnavnet for et revisjonssporingsarkiv for arbeidsstasjon formatet `WorkstationAuditTrailData-<workstation name>>-<YYYY><MMDDHHMMSS>.atds`.

Denne prosedyren kan også brukes til å åpne et revisjonsspor for en resultattabell.

1. Åpne Audit Trail-arbeidsområdet.
2. Klikk på **Browse (Bla gjennom)**.
3. Bla til og velg det arkiverte revisjonssporet som skal åpnes, og klikk deretter på **OK**.

Merk: Hvis du vil åpne revisjonssporet for en resultattabell, velger du den tilknyttede `qsession`-filen.

Skrive ut et revisjonsspor

1. Åpne Audit Trail-arbeidsområdet.
2. Velg revisjonssporet som skal skrives ut.
3. Klikk på **Print (Skriv ut)**.
Dialogboksen Print åpnes.
4. Velg skriveren, og klikk på **OK**.

Eksporter revisjonssporoppføringer

1. Åpne Audit Trail-arbeidsområdet.
2. Velg revisjonssporet som skal eksporteres.
3. Klikk på **Export (Eksporter)**.
4. Bla til stedet der den eksporterte filen skal lagres, skriv inn en **File Name (Filnavn)**, og klikk deretter på **Save (Lagre)**.
Revisjonssporet lagres som en csv-fil (kommaseparert verdi).

Revisjonssporregistreringer

Denne delen beskriver feltene i revisjonssporoppføringene.

Arbeidsstasjons- og prosjektrevisjonsstier er krypterte filer.

Merk: Arbeidsstasjoners revisjonsspor og arkiver er lagret i mappen `Program Data\SCIEX\Audit Data`. Prosjektets revisjonsspor og arkiver er lagret i mappen `Audit Data` for prosjektet.

Tabell 7-5: Revisjonsoppføringsfelter

Etikett	Beskrivelse
Tidsstempel	Datoen og klokkeslettet da oppføringen ble generert.
Hendelsesnavn	Navnet på hendelsen.
Beskrivelse	En beskrivelse av hendelsen.
Reason (Årsak)	Årsaken oppgitt for hendelsen.
E-signatur	Om en e-signatur ble lagt inn for hendelsen.
Full User Name (Fullt brukernavn)	Navnet på brukeren.

Tabell 7-5: Revisjonsoppføringsfelter (fortsatt)

Etikett	Beskrivelse
	Merk: For aktiviteter som utløses av en beslutningsregel, er dette brukeren som sendte inn batchen.
User (Bruker)	Bruker-ID-en til brukeren som startet hendelsen som produserte oppføringen.
Kategori	Funksjonen eller kategorien som hendelsen tilhører.

Den nederste ruten i Audit Trail-arbeidsområdet viser detaljert informasjon om en valgt aktivitet, inkludert detaljer om eventuelle endringer, hvis aktuelt.

For lister over alle hendelsene som registreres i arbeidsstasjonen og prosjektets revisjonsspor, se avsnittene: [Revisjonsspor for arbeidsstasjon](#) og [Revisjonsspor for prosjekt](#).

CAC Revisjonssporoppføringer

Denne delen beskriver feltene i revisjonssporoppføringene.

CAC og prosjektrevisjonsstier er krypterte filer.

Merk: CAC revisjonsspor og arkiver er lagret i mappen `Program Data\SCIEX\Audit Data`. Prosjektets revisjonsspor og arkiver er lagret i mappen `Audit Data` for prosjektet.

Tabell 7-6: Revisjonsoppføringsfelter

Etikett	Beskrivelse
Tidsstempel	Datoen og klokkeslettet da oppføringen ble generert.
Hendelsesnavn	Navnet på hendelsen.
Beskrivelse	En beskrivelse av aktiviteten.
Reason (Årsak)	Årsaken oppgitt for arrangementet.
E-signatur	Om en e-signatur ble lagt inn for arrangementet.
Full User Name (Fullt brukernavn)	Navnet på brukeren. Merk: For aktiviteter som utløses av en beslutningsregel, er dette brukeren som sendte inn batchen.
User (Bruker)	Bruker-ID-en til brukeren som startet hendelsen som produserte oppføringen.
Kategori	Funksjonen eller kategorien som hendelsen tilhører.

Den nederste ruten i arbeidsområdet Audit Trail viser detaljert informasjon om en valgt aktivitet, inkludert detaljer om eventuelle endringer, hvis aktuelt.

For lister over alle hendelsene som er registrert i CAC og prosjektets revisjonsspor, se avsnittene: [Tabell 3](#) og [Revisjonsspor for prosjekt](#).

Revisjonssporarkiver

Revisjonsoppføringene akkumuleres i Project Audit Trail og Workstation Audit Trail, og kan utgjøre store filer som er vanskelige å navigere i og administrere.

Når et revisjonsspor når 20 000 oppføringer, arkiveres det. En endelig arkivpost legges til i revisjonssporet, og deretter lagres revisjonssporet med et navn som angir type revisjonsspor og dato og klokkeslett. Et nytt revisjonsspor opprettes. Den første oppføringen i det nye revisjonssporet angir at revisjonssporet er arkivert, og angir banen til det arkiverte revisjonssporet.

Arbeidsstasjon revisjonssporarkiver lagres i mappen `C:\ProgramData\SCIEX\Audit Data`. Filnavnene er i formatet `WorkstationAuditTrailData-<workstation name>-<YYYY><MMDDHHMMSS>.atds`. For eksempel `WorkstationAuditTrailData-SWDSXPT158-20190101130401.atds`.

Prosjektets revisjonsspor og arkiver er lagret i mappen `Audit Data` for prosjektet.

Windows-tillatelser

A

Dette avsnittet inneholder en liste over Windows-tillatelsene som kreves for hver brukerrolle og for SYSTEMBRUKEREN, for korrekt bruk av SCIEX OS-programvaren.

Merk: Standardbanen for den *Installed Root Directory*-mappen er D:\SCIEX OS Data.

Tabell A-1: *Installed Root Directory*-mappen

Privilegium	Administrator, SYSTEM	Analytiker, metodeutvikler, vurderer
Full control	Tillat	—
Traverse folder / execute file	Tillat	Tillat
List folder / read data	Tillat	Tillat
Read attributes	Tillat	Tillat
Read extended attributes	Tillat	Tillat
Create files / write data	Tillat	Tillat
Create folders / append data	Tillat	Tillat
Write attributes	Tillat	Tillat
Write extended attributes	Tillat	Tillat
Delete subfolders and files	Tillat	—
Delete	Tillat	—
Read permissions	Tillat	Tillat
Change permissions	Tillat	—
Take ownership	Tillat	—

Tabell A-2: *Installed Root Directory\TempData*-mappen

Privilegium	Administrator, SYSTEM	Analytiker, metodeutvikler, vurderer
Full control	Tillat	—
Traverse folder / execute file	Tillat	Tillat
List folder / read data	Tillat	Tillat
Read attributes	Tillat	Tillat

Tabell A-2: *Installed Root Directory\TempData*-mappen (fortsatt)

Privilegium	Administrator, SYSTEM	Analytiker, metodeutvikler, vurderer
Read extended attributes	Tillat	Tillat
Create files / write data	Tillat	Tillat
Create folders / append data	Tillat	Tillat
Write attributes	Tillat	Tillat
Write extended attributes	Tillat	Tillat
Delete subfolders and files	Tillat	Tillat
Delete	Tillat	Tillat
Read permissions	Tillat	Tillat
Change permissions	Tillat	—
Take ownership	Tillat	—

Tabell A-3: *C:\ProgramData\SCIEX\Audit Data*-mappen

Privilegium	Administrator, SYSTEM	Analytiker, metodeutvikler, vurderere
Full control	Tillat	—
Traverse folder / execute file	Tillat	Tillat
List folder / read data	Tillat	Tillat
Read attributes	Tillat	Tillat
Read extended attributes	Tillat	Tillat
Create files / write data	Tillat	Tillat
Create folders / append data	Tillat	Tillat
Write attributes	Tillat	Tillat
Write extended attributes	Tillat	Tillat
Delete subfolders and files	Tillat	—
Delete	Tillat	—
Read permissions	Tillat	Tillat
Change permissions	Tillat	—
Take ownership	Tillat	—

Revisjonshendelser

B

Dette avsnittet viser revisjonshendelser i SCIEX OS. Den viser også de tilsvarende revisjonshendelsene i Analyst-programvaren for brukere som migrerer fra Analyst-programvaren til SCIEX OS.

Revisjonsspor for prosjekt

Hvert prosjekt har et revisjonsspor. Prosjektets revisjonsspor er lagret i mappen `Audit Data` for prosjektet. Revisjonssporfilnavnet er `ProjectAuditEvents.atds`.

Merk: Standardrevisjonskart for nye prosjekter som er opprettet i Central Administrator Console (CAC)-programvaren er Silent Audit Map.

Hendelser i prosjektrevisjonsspor vises i både CAC-programvaren og SCIEX OS.

Tabell B-1: Revisjonssporhendelser for prosjekt

SCIEX OS eller CAC	Analyst-programvare
Analytics-arbeidsområde	
Faktisk konsentrasjon er endret	Kvantifiseringshendelser: 'Concentration' has been changed
Autodata er eksportert	—
Automatisk rapport opprettet	—
Automatisk behandling av fil lagret	—
Strekkode-ID er endret	—
Sammenligningsprøve endret i ikke-måltrettet arbeidsflyt	—
Egendefinerte kolonner endret	Kvantifiseringshendelser: 'Custom Title' has changed
DataUTForskning åpnet	Prosjekthendelser: Data File has been opened
Data eksportert	—
Data overført til LIMS	—
Fortynningsfaktor	Kvantifiseringshendelser: 'Dilution Factor' has been changed
Ekstern kalibrering er endret	—
Ekstern kalibrering er eksportert	—

Tabell B-1: Revisjonssporhendelser for prosjekt (fortsatt)

SCIEX OS eller CAC	Analyst-programvare
Fil lagret	Prosjekthendelser: Quantitation Results Table has been created, Quantitation Results Table has been modified, Kvantifiseringshendelser: Results Table has been saved.
Formelkolonnen er endret	Kvantifiseringshendelser: Formula name has been changed, Formula name has been added, Formula string has been changed, Formula column has been removed
Integrering klarert	—
Integreringsparametere er endret	Kvantifiseringshendelser: Quantitation peak has been integrated
Søkeresultat for bibliotek er endret	—
Manuell integrering	Kvantifiseringshendelser: Quantitation Peak has been integrated
Manuell integrering tilbakeført	Kvantifiseringshendelser: Quantitation peak has been reverted back to original
MS/MS-valg er endret	—
Behandlingsmetode endret og anvendt	Kvantifiseringshendelser: Quantitation method has been changed
Behandlingsmetode skrevet ut	—
Behandlingsmetode lagret	—
Endrede standardinnstillinger for prosjektet	—
Rapport opprettet	Prosjekthendelser: Printing document on printer, Finished printing document on printer
Resultattabell er godkjent	Kvantifiseringshendelser: QA reviewer has accessed a results table
Resultattabell er opprettet	Kvantifiseringshendelser: Results table has been created
Resultattabell er låst	—
Resultattabell er gjennomgått	—
Resultattabell er låst opp	—

Tabell B-1: Revisjonssporhendelser for prosjekt (fortsatt)

SCIEX OS eller CAC	Analyst-programvare
Prøve-ID er endret	Kvantifiseringshendelser: 'Sample ID' has been changed
Prøvenavn er endret	Kvantifiseringshendelser: 'Sample Name' has been changed
Prøvetype er endret	Kvantifiseringshendelser: 'Sample Type' has been changed
Prøver lagt til eller fjernet	Kvantifiseringshendelser: Files have been added to Results Table, Files have been removed from Results Table, Samples have been added/removed
Std. Addisjon faktisk konsentrasjon endret	—
Valg av brukt kolonne endret	Kvantifiseringshendelser: 'Use IT' has been changed
Vekt/volum er endret	'Weight to Volume Ratio' has been changed
Vindu/rute skrevet ut	Prosjekthendelser: Printing document on printer, Finished printing document on printer
Audit Map-side	
Revisjonskart for prosjekt er endret	Prosjekthendelser: Project Settings have been changed
Revisjonsspor for prosjekt er eksportert	—
Revisjonsspor for prosjekt er skrevet ut	—
Batch-arbeidsområde	
Batchinformasjon importert fra LIMS/text	—
Batch lagret	—
Batch sendt inn	Instrumenthendelser: Batch file submitted
Print (Skriv ut)	Prosjekthendelser: Printing Document on printer, Finished printing document on printer
Explorer-arbeidsområde⁴	
Åpen/åpne prøve(r)	Prosjekthendelser: Data File has been opened

⁴ Explorer-hendelser blir registrert i prosjektrevisjonssporet når brukere bruker data i det aktive prosjektet.

Tabell B-1: Revisjonssporhendelser for prosjekt (fortsatt)

SCIEX OS eller CAC	Analyst-programvare
Print (Skriv ut)	Prosjekthendelser: Printing Document on printer, Finished printing document on printer
Rekalibrerer prøve(r)	—
Rekalibrering av prøve(r) er startet	—
LC Method (LC-metode)-arbeidsområde	
LC-metode er lagret	—
Print (Skriv ut)	Prosjekthendelser: Printing Document on printer, Finished printing document on printer
MS Method (MS-metode)-arbeidsområde	
MS-metode er lagret	—
Print (Skriv ut)	Prosjekthendelser: Printing Document on printer, Finished printing document on printer
Queue-arbeidsområde	
Prøveinnhenting er fullført	—
Prøve redigert	—
Prøve starter å innhente	—
Prøve overført	—

Revisjonsspor for arbeidsstasjon

Hver arbeidsstasjon har ett revisjonsspor for arbeidsstasjonen. Arbeidsstasjonens revisjonsspor er lagret i mappen `Program Data\SCIEX\Audit Data`. Revisjonssporfilnavnet er i formatet: `WorkstationAuditTrailData.atds`.

Merk: Standardrevisjonsskart for nye arbeidsstasjoner i Central Administrator Console (CAC)-programvaren er **Silent Audit Map**.

Revisjonssporingshendelser vises i både CAC-programvaren og i SCIEX OS.

Tabell B-2: Revisjonssporhendelser for arbeidsstasjon

SCIEX OS	Analyst-programvare
Audit Map	
Revisjonsskart for arbeidsstasjon er endret	Instrumenthendelser: Instrument Settings have been changed

Tabell B-2: Revisjonssporhendelser for arbeidsstasjon (fortsatt)

SCIEX OS	Analyst-programvare
Revisjonsspor for arbeidsstasjon er eksportert	—
Revisjonsspor for arbeidsstasjon er skrevet ut	—
CAC	
Sentraladministrasjon aktivert/deaktivert	—
Innstillinger for sentraladministrasjon hentet/kunne ikke hentes	—
Kontrollsum for datafil	
Kontrollsum for WIFF-datafil er endret	—
Explorer-arbeidsområde⁵	
Åpen/åpne prøve(r)	Prosjekthendelser: Data File has been opened
Print (Skriv ut)	Prosjekthendelser: Printing document on printer, Finished printing document on printer
Rekalibrerer prøve(r)	—
Rekalibrering av prøve(r) er startet	—
Hardware Configuration (Maskinvarekonfigurasjon)	
Enheter aktivert	Instrumenthendelser: Hardware profile has been activated
Enheter deaktivert	Instrumenthendelser: Hardware profile has been deactivated
Instrumentinnstilling	
Automatisk MS Tuning-oppdatering	Instrumenthendelser: Tune parameter settings changed
Fastvare er endret	—
MS-tuningendringer	Instrumenthendelser: Tune parameter settings changed
Resultat av utskriftsprosedyre i MS Tune	Prosjekthendelser: Printing Document on printer, Finished printing document on printer

⁵ Explorer-hendelser blir registrert i arbeidsstasjonens revisjonsspor når brukere bruker data som ikke er i det aktive prosjektet.

Tabell B-2: Revisjonssporhendelser for arbeidsstasjon (fortsatt)

SCIEX OS	Analyst-programvare
Queue-arbeidsområde	
Automatisk injeksjon oppstått	—
Automatisk reinjeksjon oppstod	—
Batch flyttet i kø	Instrumenthendelser: Move Batch
Utskriftskø	Prosjekthendelser: Printing Document on printer, Finished printing document on printer
Henter inn prøver på nytt	Instrumenthendelser: Reacquiring sample(s)
Prøveinnhenting er fullført	Prosjekthendelser: Sample has been added to Data file
Prøve flyttet i kø	Instrumenthendelser: Sample moved from position x to position y of Batch File
Prøve starter å innhente	—
Security (Sikkerhet)	
Automatisk utlogging etter system	Instrumenthendelser: User Logged out
Tvunget avlogging av en annen bruker	Instrumenthendelser: User Logged out
Tvungen avlogging mislykket	—
Skjermopplåsing mislyktes	—
Påloggingsinformasjon for sikker nettverkskonto er endret	Instrumenthendelser: Acquisition Account Changed
Påloggingsinformasjon for sikker nettverkskonto er fjernet	Instrumenthendelser: Acquisition Account Changed
Påloggingsinformasjon for sikker nettverkskonto er angitt	Instrumenthendelser: Acquisition Account Changed
Sikkerhetskonnfigurasjon er endret	Instrumenthendelser: The Security Configuration has been modified, Screen Lock Changed, Auto Logout changed
Bruker lagt til/slettet	Instrumenthendelser: User Added, User Deleted
Bruker har logget på	Instrumenthendelser: User Logged In
Bruker har logget av	Instrumenthendelser: User Logged out
Bruker har slått av eksklusiv modus	—
Brukerinnloggingen mislyktes	Instrumenthendelser: User Login Failed

Tabell B-2: Revisjonssporhendelser for arbeidsstasjon (fortsatt)

SCIEX OS	Analyst-programvare
Innstillingene for brukeradministrasjon er eksportert	—
Innstillingene for brukeradministrasjon er importert	—
Innstillingene for brukeradministrasjon er gjenopprettet	—
Brukerrolle tilordnet til bruker/brukergruppe	Instrumenthendelser: User Changed User Type
Brukerrolle slettet	Instrumenthendelser: User Type Deleted
Brukerrolle endret	Instrumenthendelser: User Type Changed
Nettbruker har logget på (ikke i bruk)	—
Nettbruker har logget ut (ikke i bruk)	—
Brukerlogg	
Skriv ut hendelseslogg	—

Tabell B-3: Revisjonssporhendelser for CAC

CAC	Analyst-programvare
Audit Map-side	
Revisjonskart for arbeidsstasjon er endret	Instrumenthendelser: Instrument Settings have been changed
Revisjonsspor for arbeidsstasjon er eksportert	—
Revisjonsspor for arbeidsstasjon er skrevet ut	—
CAC	
CAC-innstillinger er eksportert	—
CAC-innstillinger er importert	—
CAC-innstillinger er gjenopprettet	—
Prosjektinnstillinger aktivert/deaktivert i en arbeidsgruppe	—
Prosjekt tilordnet/ikke-tilordnet til en arbeidsgruppe	—
Sikkerhetstillatelse lagt til for sentral administrasjon	—

Tabell B-3: Revisjonssporhendelser for CAC (fortsatt)

CAC	Analyst-programvare
Bruker lagt til/slettet	—
Brukerrolle lagt til	—
Brukerrolle slettet	—
Brukerrolle endret	—
Brukerrolle(r) tilordnet/ikke tilordnet til bruker(e) i arbeidsgruppe	—
Bruker(e)/brukergruppe(r) er tilordnet/ikke-tilordnet en arbeidsgruppe	—
Arbeidsgruppe lagt til/slettet	—
Arbeidsgruppe omdøpt	—
Arbeidsstasjon(er) tilordnet/ikke tilordnet til en arbeidsgruppe	—
Sikkerhet	
Automatisk utlogging etter system	Instrumenthendelser: User Logged out
Tvunget avlogging av en annen bruker	Instrumenthendelser: User Logged out
Tvungen avlogging mislykket	—
Skjermopplåsing mislyktes	—
Påloggingsinformasjon for sikker nettverkskonto er endret	Instrumenthendelser: Acquisition Account Changed
Påloggingsinformasjon for sikker nettverkskonto er fjernet	Instrumenthendelser: Acquisition Account Changed
Påloggingsinformasjon for sikker nettverkskonto er angitt	Instrumenthendelser: Acquisition Account Changed
Sikkerhetskonnfigurasjon er endret	Instrumenthendelser: The Security Configuration has been modified, Screen Lock Changed, Auto Logout changed
Bruker lagt til/slettet	Instrumenthendelser: User Added, User Deleted
Bruker har logget på	Instrumenthendelser: User Logged In
Bruker har logget av	Instrumenthendelser: User Logged out
Bruker har slått av eksklusiv modus	—
Brukerinnloggingen mislyktes	Instrumenthendelser: User Login Failed

Tabell B-3: Revisjonssporhendelser for CAC (fortsatt)

CAC	Analyst-programvare
Innstillingene for brukeradministrasjon er eksportert	—
Innstillingene for brukeradministrasjon er importert	—
Innstillingene for brukeradministrasjon er gjenopprettet	—
Bruker eller gruppe aktivert	—
Bruker eller gruppe deaktivert	—
Brukerrolle tilordnet til bruker/brukergruppe	Instrumenthendelser: User Changed User Type
Brukerrolle slettet	Instrumenthendelser: User Type Deleted
Brukerrolle endret	Instrumenthendelser: User Type Changed
Nettbruker har logget på (ikke i bruk)	—
Nettbruker har logget ut (ikke i bruk)	—
Brukerlogg	
Skriv ut hendelseslogg	—

Tilordning av tillatelser mellom Analyst- og SCIEX OS-programvaren

C

Dette avsnittet er for brukere som migrerer fra Analyst-programvaren til SCIEX OS-programvaren, for å hjelpe dem med å migrere brukerens sikkerhetsinnstillinger. Den viser tillatelsene i Analyst-programvaren som tilsvarer tillatelsene i SCIEX OS-programvaren.

Tabell C-1: Tilordning av tillatelse

SCIEX OS-programvare	Analyst-programvare
Batch-arbeidsområde	
Send inn ulåste metoder	—
Open (Åpne)	Batch: Open Existing Batches
Save As (Lagre som)	Batch: Create New Batches, Import, Edit Batches, Save Batches, Overwrite Batches
Submit (Send inn)	Batch: Submit Batches
Save (Lagre)	Batch: Save Batches, Overwrite Batches
Lagre ionereferansetabell	—
Legg til undermapper for data	—
Konfigurer beslutningsregler	—
Overskriv batch	Overwrite batches
Send inn batch før lagring	—
Configuration-arbeidsområde	
Generell fane	—
Generelt: endre regional innstilling	—
Generelt: fullskjermmodus	—
Generelt: Stopp Windows-tjenester	—
LIMS-kommunikasjonsfane	—
Fane for revisjonskart	Audit Trail Manager (Styringsprogram for revisjonsspor): Change Audit Trail Settings, Create or Modify Audit Maps
Kø-fane	—
Kø: instrumentets inaktive tid	—

Tilordning av tillatelser mellom Analyst- og SCIEX OS-programvaren

Tabell C-1: Tilordning av tillatelse (fortsatt)

SCIEX OS-programvare	Analyst-programvare
Kø: maks. antall innsamlede prøver	—
Kø: andre køinnstillinger	—
Prosjekter-fane	—
Prosjekter: opprett prosjekt	Analyst Application: Create Project
Prosjekter: bruk en revisjonskartmal på et eksisterende prosjekt	Audit Trail Manager: Change Audit Trail Settings
Prosjekter: opprett rotkatalog	Analyst Application: Create Root Directory
Prosjekt: angi gjeldende rotkatalog	Analyst Application: Set Root Directory
Prosjekter: spesifiser nettverkslegitimasjon	—
Prosjekter: Aktiver kontrollsumskrivning for oppretting av wiff-data	—
Prosjekter: tøm rotkatalog	—
Enhetsfane	Maskinvarekonfigurasjon: Create, Delete, Edit, Activate/Deactivate
Brukeradministrasjon-fane	Security Config
Tving avlogging av bruker	Unlock/Logout Application
CAC-fane ³	—
Fanen utskriftsmal:	—
Utskriftsmaler: Opprett og endre utskriftsmaler	—
Utskriftsmaler: Angi standard utskriftsmal	—
Utskriftsmaler: Bruk gjeldende mal på alle prosjekter i rotkatalogen	—
Event Log-arbeidsområde	
Tilgang til arbeidsområdet for hendelseslogg	—
Arkivlogg	—
Audit Trail-arbeidsområde	

³ I versjon 3.1 ble tillatelsen **Aktiver sentraladministrasjon** omdøpt til **CAC**. CAC-siden i Configuration-arbeidsområdet kan brukes til å konfigurere sentral administrasjon av SCIEX OS-programvaren.

Tabell C-1: Tilordning av tillatelse (fortsatt)

SCIEX OS-programvare	Analyst-programvare
Tilgang til arbeidsområdet for revisjonsspor	Audit Trail Manager: View Audit Trail Data
Vis aktivt revisjonskart	Audit Trail Manager: View Audit Trail Data
Skriv ut/eksporter revisjonsspor	Audit Trail Manager: View Audit Trail Data
Datainnsamlingspanel	
Start	—
Stopp	—
Save (Lagre)	—
MS Method- og LC Method-arbeidsområder	
Tilgangsmetode for arbeidsområde	—
Nytt	Innhentingsmetode: Create/Save acquisition method
Open (Åpne)	Innhentingsmetode: Open acquisition method as read-only (acquire mode)
Save (Lagre)	Innhentingsmetode: Overwrite acquisition methods, Create/Save acquisition method
Save As (Lagre som)	Innhentingsmetode: Overwrite acquisition methods, Create/Save acquisition method
Låse-/opplåsningsmetode	—
Overwrite acquisition methods (Overskrive innsamlingsmetoder)	Overwrite acquisition methods
Queue-arbeidsområde	
Administrer	Sample Queue: Reacquire, Delete Sample or Batch, Move Batch
Start/Stopp	Sample Queue: Start Sample, Stop Sample, Abort Sample, Stop Queue
Print (Skriv ut)	Report Template Editor: Print
Rediger prøve	—
Library-arbeidsområde	
Tilgang til bibliotekets arbeidsområde	Explore: Setup library location, Setup library user options, Add library record, Add spectrum to library, Modify library record (overrides add/delete if disabled), Delete MS spectrum, Delete UV spectrum,

Tilordning av tillatelser mellom Analyst- og SCIEX OS-programvaren

Tabell C-1: Tilordning av tillatelse (fortsett)

SCIEX OS-programvare	Analyst-programvare
	Delete structure, View library, Search library
MS Tune-arbeidsområde	
Tilgang til MS Tune-arbeidsområdet	—
Avansert MS-tuning	Tune (Tuning): Instrument Optimization, Manual Tune, Edit Tuning Options
Avansert feilsøking	—
Hurtig statuskontroll	Tune: Instrument Opt
Gjenopprett instrumentdata	Tune: Edit Tuning Options, Edit instrument data
Analytics-arbeidsområde	
Nye resultater	Kvantifisering: Create new results tables
Opprett behandlingsmetoder	Kvantifisering: Create quantitation methods
Endre behandlingsmetode	Kvantifisering: Modify existing methods
Allow Export and Create Report of unlocked Results Table (Tillat eksport og opprett rapport om ulåste resultattabeller)	—
Lagre resultater for automatiseringsbatch	—
Change default quantitation method integration algorithm (Endre standardalgoritme for integrering av) kvantifiseringsmetoder	Kvantifisering: Change default method options
Change default quantitation method integration parameters (Endre standardparametre for integrering av kvantifiseringsmetoder)	Kvantifisering: Change default method options
Aktiver prosjektmodifisert toppadvarsel	—
Legg til prøver	Kvantifisering: Add and Remove samples from results table
Fjern valgte prøver	Kvantifisering: Add and Remove samples from results table
Eksporter, importer eller fjern ekstern kalibrering	—
Endre prøvenavn	Kvantifisering: Modify sample name

Tabell C-1: Tilordning av tillatelse (fortsett)

SCIEX OS-programvare	Analyst-programvare
Endre prøvetype	Kvantifisering: Modify Sample Type
Endre prøve-ID	Kvantifisering: Modify Sample ID
Endre faktisk konsentrasjon	Kvantifisering: Modify Analyte Concentration
Endre fortynningsfaktor	Kvantifisering: Modify Dilution Factor
Endre kommentarfelt	Kvantifisering: Modify Sample Comment
Aktiver manuell integrering	Kvantifisering: Manually integrate
Sett topp til 'Ikke funnet'	—
Inkluder eller ekskluder en topp fra resultattabellen	Kvantifisering: Exclude standards from calibration
Regresjonsalternativer	Kvantifisering: Change regression parameters
Endre integreringsparametre for resultattabell for et enkelt kromatogram	Kvantifisering: Change "simple" parameters in peak review, Change "advanced" parameters in peak review
Endre kvantifiseringsmetode for resultattabell-komponenten	Kvantifisering: Edit results tables' method
Opprett nye innstillinger for metrisk diagram	Kvantifisering: Modify or create metric plot settings
Legg til egendefinerte kolonner	Kvantifisering: Create or modify formula columns
Angi tittelformat for gjennomgang av topper	—
Remove custom column (Fjern egendefinert kolonne)	Kvantifisering: Create or modify formula columns
Visningsinnstillinger for resultattabell	Kvantifisering: Change results table column precision, Change results table column visibility, Modify results table settings
Lås resultattabell	—
Lås opp resultattabell	—
Merk resultatfilen som gjennomgått og lagre	—
Endre rapportmal	Report Template Editor: Create/Modify report templates

Tilordning av tillatelser mellom Analyst- og SCIEX OS-programvaren

Tabell C-1: Tilordning av tillatelse (fortsatt)

SCIEX OS-programvare	Analyst-programvare
Overfør resultater til LIMS	—
Endre strekkodekolonne	—
Endre sammenligningsprøvetildeling	—
Legg til MSMS-spektra i biblioteket	Explore: Add spectrum to library record
Prosjektets standardinnstillinger	Kvantifisering: Modify global (default) settings
Opprett rapport i alle formater	—
Rediger parametere for flaggingskriterier	—
Parameterendring for automatisk fjerning av avvik	—
Aktiver automatisk fjerning av avvik	—
Oppdater behandlingsmetode via FF/LS	—
Oppdater resultater via FF/LS	—
Aktiver gruppering etter addukt-funksjonalitet	Kvantifisering: Create Analyte Groups, Modify Analyte Groups
Bla etter filer	—
Aktiver standardtilføyelse	—
Angi prosentregel for manuell integrering	Kvantifisering: Enable or Disable percent rule in Manual Integration
Vekt/volum	Kvantifisering: Modify Weight To Volume ratio
Overskriv en resultattabell	When saving, replace existing results tables
Merk resultatfilen som godkjent og lagre	—
Central Monitoring-arbeidsområde	
Fanen tilgangskø	—
Utskriftskø	—
Start/stopp kø	—
Explorer-arbeidsområde	
Tilgang til arbeidsområde for UTForsker	—
Export (Eksporter)	Explore: Save data to text file
Print (Skriv ut)	Report Template Editor: Print

Tabell C-1: Tilordning av tillatelse (fortsatt)

SCIEX OS-programvare	Analyst-programvare
Options (Alternativer)	—
Kalibrer på nytt	Tune: Calibrate from current spectrum
Bla etter filer	—

Sjekksum for datafiler

D

Merk: Fordi `wiff2-filer` har innebygde dataintegritetsmekanismer, som inkluderer kryptering og intern validering, er det ikke nødvendig med en ekstern sjekksum. Det er derfor ikke obligatorisk å aktivere kontrollsumfunksjonen for `wiff2`-filer.

Vi anbefaler at du aktiverer funksjonen for datafilsjekksum for `wiff`-filer. Sjekksumfunksjonen er en syklisk redundanssjekk for å bekrefte datafilens integritet.

Hvis funksjonen datafilsjekksum er aktivert, bruker programvaren en offentlig MD5-krypteringsalgoritme til å generere en sjekksumverdi når brukeren oppretter en datafil (`wiff`). Verdien er lagret i filen. Når du bekrefter sjekksummen, vil programvaren beregne sjekksummen og sammenligne den beregnede sjekksummen med sjekksummen som er lagret i filen.

Sammenligningen av sjekksummen kan ha tre utfall:

- Hvis verdiene stemmer overens, er sjekksummen gyldig.
- Hvis verdiene ikke stemmer overens, er sjekksummen ugyldig. En ugyldig sjekksum er en indikasjon på at filen ble endret eksternt eller at filen ble lagret da beregningen av sjekksummen ble aktivert og sjekksummen er forskjellig fra den opprinnelige sjekksummen.
- Hvis filen ikke har noen lagret sjekksumverdi, blir ikke sjekksummen funnet. En sjekksumverdi beholdes ikke i filen hvis filen ble lagret da funksjonen for datafilsjekksum ble deaktivert.

Merk: Brukeren kan bruke Analyst-programvaren for å utføre en sjekk av sjekksummen. Se dokumentasjonen for Analyst-programvaren.

Aktiver eller deaktiver datafilens sjekksumfunksjon

1. Åpne Configuration-arbeidsområdet.
2. Klikk på **Projects (Prosjekter)**.
3. Utvid om nødvendig **Datafilsikkerhet**.
4. For å aktivere datafilkontrollsumfunksjonen merker du av i avmerkingsboksen **Aktiver kontrollsumskriving for oppretting av wiff-data**. Fjern merket i denne avmerkingsboksen for å deaktivere funksjonen.

Kontakt oss

Adresser



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

UKRP

Leica Microsystems (UK) Ltd.
19 Jessops Riverside
800 Brightside Lane, Sheffield
S9 2RX, England



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

SCIEX Hovedkvarter

AB Sciex LLC
250 Forest Street
Marlborough, MA 01752
USA

Kundeopplæring

- Globalt: sciex.com/contact-us

Online læresenter

- [SCIEX Now Learning Hub](#)

SCIEX-støtte

SCIEX og deres representanter har en global stab av utdannede og kvalifiserte servicespesialister og tekniske spesialister. De kan svare på spørsmål om systemet eller tekniske problemer som kan oppstå. For mer informasjon, gå til SCIEX-nettstedet på sciex.com eller bruk en av lenkene som følger for å kontakte oss.

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

Cybersikkerhet

De siste retningslinjene for cybersikkerhet for SCIEX-produkter finner du på sciex.com/productsecurity.

Dokumentasjon

Denne versjonen av dokumentet overgår alle tidligere versjoner av dette dokumentet.

Det kreves Adobe Acrobat Reader for å se dette dokumentet elektronisk. Hvis du vil laste ned siste versjon, gå til <https://get.adobe.com/reader>.

Se versjonsmerknadene eller installasjonsveiledningen som følger med programvaren for dokumentasjon om programvareproduktet.

Du finner produktdokumentasjon for maskinvare i dokumentasjonen som følger med systemet eller komponenten.

De siste versjonene av dokumentasjonen er tilgjengelige fra SCIEX-nettstedet på sciex.com/customer-documents.

Merk: Hvis du ønsker en gratis, trykt versjon av dette dokumentet, ta kontakt med sciex.com/contact-us.
