

Vejledning til Brugeradministrationsmodulet

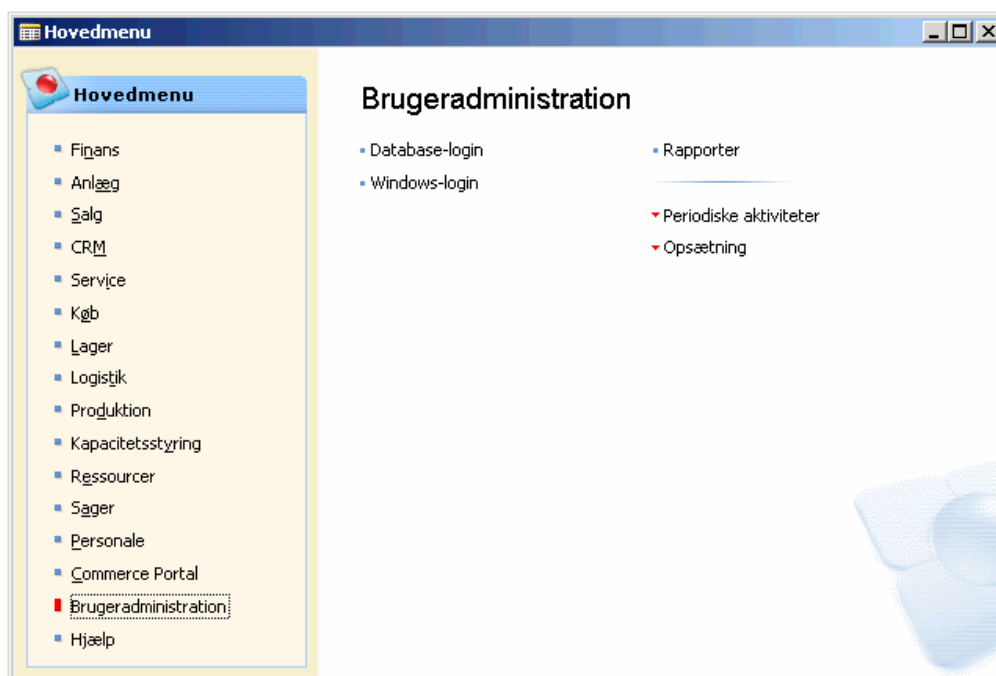
Brugeradministration	3
Indledning	3
Begreber.....	4
Forudsætninger	4
Brugeradministrationsopsætning	5
Overførsel til SQL-server	5
Windows authentication.....	6
SQL-server authentication	7
Profiler, roller og rettigheder	9
Profiler	9
Roller.....	11
Lagdeling af roller.....	15
Rettigheder	15
Betingede rettigheder	17
Eksempel på oprettelse af ny Rolle.....	19
Eksempel på oprettelse af ny Profil	20
Indlæsning af rettigheder og roller.....	22
Hvem kan oprette brugere ?.....	24
Superbruger.....	24
Funktionsansvarlige brugere	24
Brugeroprettelse.....	25
Databaselogin.....	25
Eksempel.....	26
Windowslogin	28
Eksempel.....	28
Validering	29
Eksempel.....	30
Kopiering af rettigheder	31
Eksempel på kopiering af rettigheder	31
Fejlbeskeder samt årsag	33
Ej overførsel af brugerlogin til sql-server	33
Ej tildeling af rettigheder til brugeren.....	34
Brugeren er ikke oprettet på netværket.....	34
Brugeren er oprettet i en anden database med et andet password.....	35
Sletning af en Navision Stat bruger	35
Omdøbning af en bruger	36
Ændring af superbrugerens password.....	36
Ændring af password i Navision Stat.....	38
Database login.....	38
Windows login	38
Ændring af password	38
Rapportering	40
Brugerliste.....	40
Roller pr. bruger.....	40
Rettigheder pr. Rettighedsgrp.	41
Roller pr. profil	41

Brugere pr. rolle	42
Brugere pr. objekt	42
Objekter pr. bruger.....	43
Best Practise.....	44
Anbefalinger	44
Kontrol af tildelte rettigheder.....	46
Hvad skal man være opmærksom på	46
Hvordan identificerer man de kritiske fejl.....	48

Brugeradministration

Indledning

Brugeradministrationsværktøjet i Navision Stat er lavet med henblik på at lette arbejdsgangen for de medarbejdere, der står for oprettelse og vedligeholdelse af brugere og rettigheder i Navision Stat. Formålet er at kunne styre adgang til data fra ét sted, nemlig Navision Stat. For at det kan lade sig gøre, skal de rettigheder, man får tildelt i Navision Stat, afspejle sig på SQL-serveren. Dette er specielt vigtigt for brugere, der anvender 3. parts produkter som f.eks. Crystal Reports eller MS Excel til at hente data direkte fra SQL-serveren.



Begreber

I nedenstående tabel er der lavet en oversigt over de begreber, der anvendes i Brugeradministrationsmodulet.

Begreb	Beskrivelse
Windows-login	Svarer til Unified Logon. Brugere oprettet med NT Authentication på SQL-serveren og med Windows-login i Navision Stat. Windows-login skal ikke anvende bruger-id og password ved anvendelse af Navision Stat.
Database-login	Hvis man har et Database-login, er det databasen, der verificerer brugeren. Brugeren skal være oprettet på SQL-serveren og som Database-login i Navision Stat. Ved anvendelse af Navision Stat kræves bruger-id og password.
SQL password	Ved oprettelse af et nyt Database-login oprettes der automatisk et Database-login på SQL-serveren, såfremt overførsel til server valgt. Brugeren oprettes med det password, der angives i feltet "SQL password".
Rolle	En Rolle er en samling af rettigheder til en gruppe af Navision Stat objekter (eksempelvis tabeller, formularer, kodeenheder m.m.), der hører sammen inden for et bestemt område af applikationen (f.eks. indtastning og bogføring i en kassekladde).
Profil	En Profil er en samling af roller. Anvender man automatisk overførsel, oprettes en database-rolle på serveren, hver gang der oprettes en Profil i Navision. Database-rollen får select-rettigheder (læse-rettigheder) til de samme tabeller, som rollerne (og dermed Profilen) har læserettigheder til.

I det følgende afsnit bliver ovenstående begreber og deres anvendelse anskueliggjort. Eksemplerne er lavet i følgende miljø:

- SQL 2000-serveren hedder 'FMNAVISON1\SQL2000'
- Databasen hedder 'SYS_udvikling360'
- Regnskabet er 'Stat Demo Manual 2'
- Operativsystemet på både klient og server er Windows 2000

Forudsætninger

Det er en fordel (for brugeradministratoren) at have læst Navisions brugerhåndbog Installation & System Management, Microsoft SQL-server Option samt at have kendskab til MS SQL Server 2000.

Brugeradministrationsopsætning

I Navision Stat varetages oprettelse af brugere, tildeling af rettigheder mm. fra modulet Brugeradministration. Når nye brugere oprettes i dette modul, oprettes de også automatisk som Login på SQL-serveren. Ligeledes er det muligt at overføre profiler og rettigheder til SQL-serveren. Det betyder med andre ord, at brugeroprettelse, tildeling af rettigheder, ændring af profiler mm. normalt kan foretages udelukkende med udgangspunkt i modulet Brugeradministration.

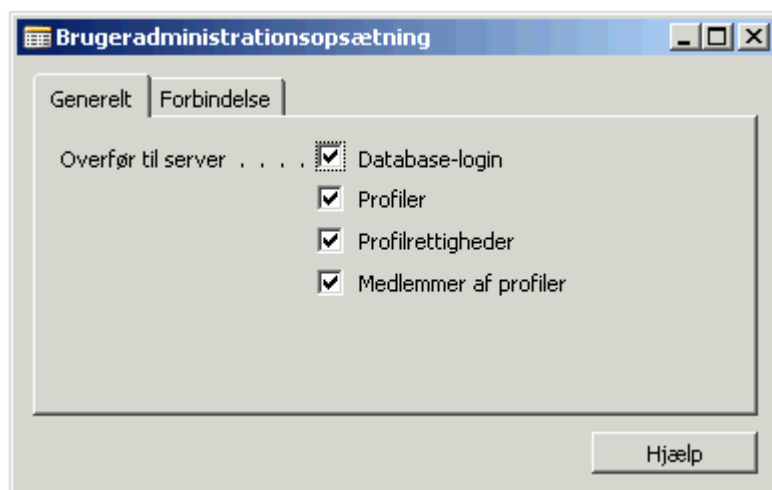
I det følgende ses på de parametre, der skal være opsat for at kunne overføre logins oprettet i Navision Stat til SQL-serveren samt de to måder (Windows authentication og SQL-server authentication), der findes i Navision Stat til oprettelse af forbindelse til SQL-serveren på.

Overførsel til SQL-server

I brugeradministrationsopsætningen er det muligt at angive hvilke data, der skal overføres til SQL-serveren.

Sti: Brugeradministration/Opsætning/Brugeradministrationsopsætning

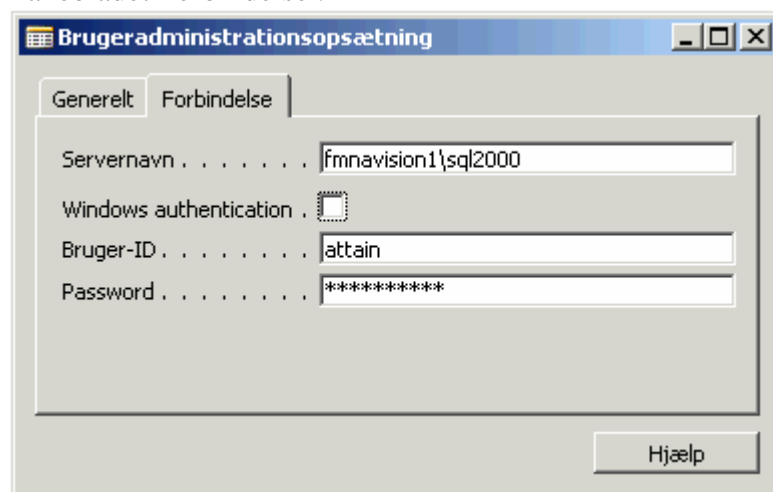
Fanebladet Generelt :



Felt	Beskrivelse
Database-login	Bevirker at brugere, der oprettes i Navision Stat, også oprettes på SQL-serveren med adgang til Navision Stat-databasen.

Profiler	Bevirker at profiler i Navision Stat oprettes som roller på SQL-serveren
Profilrettigheder	Bevirker at databaserollen på SQL-serveren får SELECT-rettigheder (dvs. læseadgang) til de tabeller som profilen har adgang til. Denne indstilling er vigtig, hvis brugerne har adgang til databasen fra andre programmer som f.eks. Excel eller Crystal Reports.
Medlemmer af profiler	Bevirker at de brugere, der oprettes og overføres fra Navision Stat, bliver medlem af de tilsvarende databaseroller på serveren. Denne indstilling er vigtig, hvis brugerne har adgang til databasen fra andre programmer som f.eks. Excel eller Crystal Reports.

Fanebladet Forbindelse :



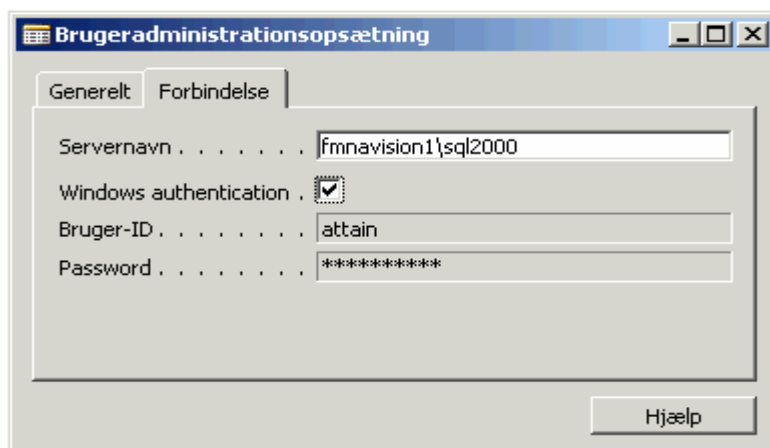
Som tidligere nævnt er der to metoder til at oprette forbindelse til SQL-serveren på. Begge metoder beskrives nærmere nedenfor.

Forbindelsen kan laves ved at anvende:

1. Windows authentication
eller
2. SQL-server authentication

Windows authentication

Windows authentication angiver, om forbindelsen til SQL-serveren skal laves på baggrund af Windows godkendelse. Ved afmærkning af feltet Windows authentication skal feltet servernavn også udfyldes.



Felt navn	Beskrivelse
Servernavn	Her skal du angive navnet på den SQL server, som Navision Stat databasen anvender.
Windows authentication	I tilfælde af at du vil oprette forbindelsen til SQL-serveren på baggrund af Windows-godkendelse, skal du markere afkrydsningsfeltet. Bemærk: Når der sættes hak i feltet Windows-authentication, kan der ikke angives Bruger-ID og Password, idet systemet her anvender data fra den bruger, der aktuelt er logget på Navision Stat.

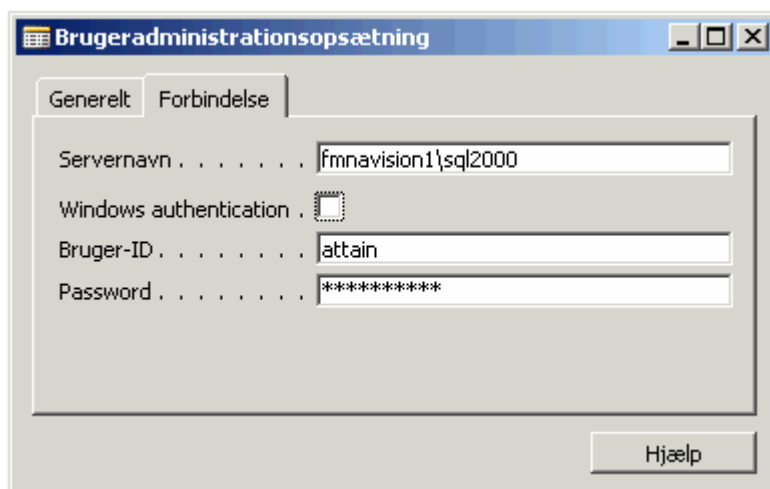
Brugere, der skal administrere brugerrettigheder i Navision, skal opfylde følgende betingelser:

- Brugeren skal være oprettet som NT User på SQL-serveren.
- Brugeren skal have Server Role 'Security Administrators' på SQL-serveren.
- Brugeren skal være dbo på databasen.

Bemærk, egenskaben dbo skal være tildelt enten via eksekvering af stored procedure sp_changedbowner eller ved at oprette forbindelsesbrugeren som System Administrator, lade forbindelsesbrugeren oprette databasen og herefter ændre hans Server Role til Security Administrator.

SQL-server authentication

I tilfælde af at der anvendes SQL-server authentication, skal der være oprettet en SQL-bruger på serveren, som er dbo på basen og har serverrollen "Security Administrator" (i dette tilfælde har SQL-brugeren Bruger-ID "attain"). Herefter skal fanebladet Forbindelse være udfyldt som vist nedenfor.



Felt navn	Beskrivelse
Servernavn	Her skal du angive navnet på den SQL-server, som Navision Stat databasen anvender.
Windows authentication	I tilfælde af at du vil oprette forbindelsen til SQL-serveren på baggrund af SQL-server authentication, skal du ikke markere afkrydsningsfeltet. Bemærk: Når der ikke sættes hak i feltet Windows-authentication, skal der angives Bruger-ID og Password, idet systemet her anvender data fra denne bruger, når der oprettes brugere i Navision Stat.
Bruger-ID	I dette felt skal du angive bruger-ID for den bruger som er dbo på basen. Denne bruger skal yderligere have serverrollen "Security Administrator". Typisk vil denne bruger være institutionens superbruger i Navision Stat.
Password	I dette felt skal du angive password for den pågældende super-bruger.

Profiler, roller og rettigheder

Profiler, roller og rettigheder er centrale begreber i brugeradministrationen i Navision Stat. Der er fra og med Navision Stat version 3.60 lagt særlig vægt på sikkerheden i form af, at der er oprettet flere rettighedslag. Brugere vil som udgangspunkt ikke kunne foretage opsætninger i de forskellige moduler med mindre brugerne specifikt tildeles rettigheder dertil.

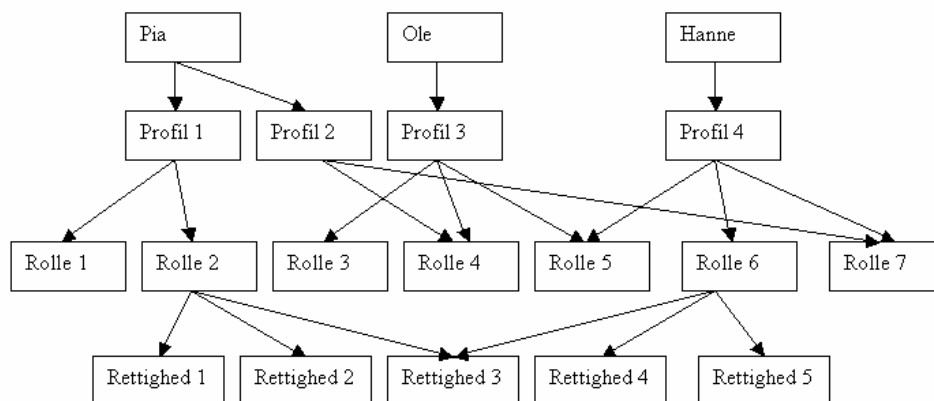
Disse rettigheder samt den yderligere opdeling gennemgås i det følgende.

Profiler

Formålet med profiler er:

- At udnytte SQL-serverens standardfunktionalitet for database-roller
- At forenkle tildelingen af roller ved at samle dem i større grupper/enheder

En profil består af en eller flere roller, hvor rollerne igen indeholder de konkrete rettigheder. Profiler kan tildeles direkte til brugerne. I Navision Stat findes en række foruddefinerede profiler, der repræsenterer nogle gængse funktionsområder i Navision Stat.



Figur 1

Sti : Brugeradministration/Opsætning/Profiler

Profil-ID	Navn
OES_BACKUP	Driftmedarbejder
OES_BASIS	Standardmedarbejder
OES_BOGHOLDER	Bogholderimedarbejder
OES_FBOGHOLDER	Funk.ansvar. bogholder
OES_FKASSERER	Funk.ansvar. kasserer
OES_FMEDARB_RED	Funk.ansvar.medarb.redigering
OES_FSL_S_OPDATER	Funk.ansvar.lønopdatering
OES_KASSERER	Kassemedarbejder
OES_MEDARB_RED	Medarbejderdata.redigering
OES_MEDARB_SE	Medarbejderdata.læsning
OES_OEKONOMI	Økonomimedarbejder
OES_OPSAET_ALMEN	Regnskabsopsætning
OES_REVISION	Revisor
OES_SLS_OPDATER	Læsning og opdat. af løndata
OES_TEKNIK	Teknisk medarbejder
OES_TIDSREG	Standardmedarbejder.tidreg.

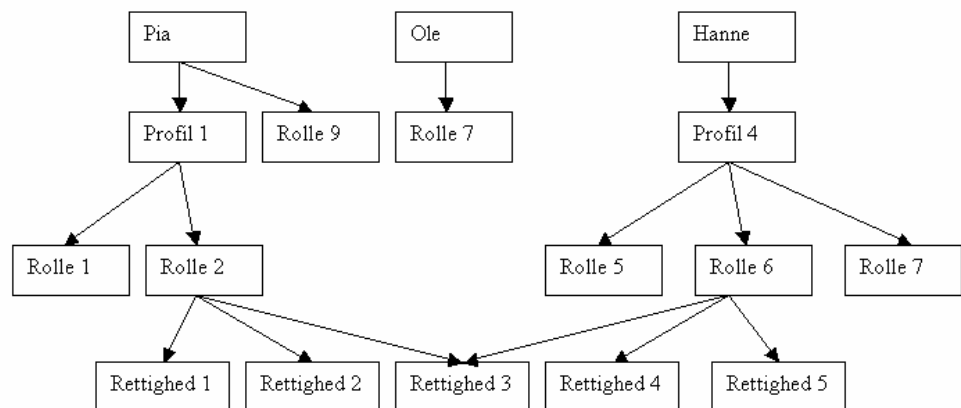
Her ses en liste med de standardprofiler, Økonomistyrelsen har oprettet til Navision Stat. I det følgende er det kort beskrevet, hvad de enkelte profiler har rettigheder til.

Profil-ID	Rettighedsbeskrivelse
OES_BACKUP	Profilen har rettigheder til at foretage back-up af Navision-databasen i Navision Stat.
OES_BASIS	Profilen har kun læseadgang til systemet.
OES_BOGHOLDER	Profilen kan udføre det meste arbejde, dog ikke kassererens arbejde eller eksempelvis foretage opsætninger.
OES_FBOGHOLDER	Profilen har de samme rettigheder som OES_BOGHOLDER, men kan dog også oprette andre brugere og tildele disse rettighederne mindre eller lig med bogholderrettigheder.
OES_FKASSERER	Profilen har de samme rettigheder som OES_KASSERER, men kan dog også oprette andre brugere og tildele disse rettighederne mindre eller lig med kassererrettigheder.
OES_FMEDARB_RED	Profilen har de samme rettigheder som OES_MEDARB_RED, men kan dog også oprette andre brugere og tildele disse rettighederne mindre eller lig med profilen OES_MEDARB_RED.

OES_FSL_S_OP DATER	Profilen har de samme rettigheder som OES_SLS_OPDATER, men kan dog også oprette andre brugere og tildele disse rettighederne mindre eller lig med profilen OES_SLS_OPDATER.
OES_KASSERE R	Profilen kan indtaste i kassererkladden og håndtere en række funktioner I forbindelse med bankmenuen.
OES_MEDARB _RED	Profilen kan redigere i personale/karriere data.
OES_MEDARB _SE	Profilen kan se i personale/karriere data.
OES_OEKONO MI	Profilen kan se data, lægge budgetter og indtaste i sags- og ressourcemodulerne.
OES_OPSAET_ ALMEN	Profilen kan foretage en række almene opsætninger i Navision Stat. Dvs en bruger med denne profil kan foretage opsætninger på tværs af modulerne.
OES_REVISION	Profilen er oprettet til brug for Rigsrevisionen. Profilen har se-rettigheder samt rettigheder til at udskrive rapporter. Profilen har dog ikke redigerings-rettigheder.
OES_SLS_OPD ATER	Profilen kan udføre den periodiske aktivitet 'Opdater medarbejderoplysninger' i personalemodulet.
OES_TEKNIK	Profilen kan indlæse hotfix's (ØS-tilretninger) og afvikle batchkørsler.
OES_TIDSREG	Profilen kan tidsregistrere i Navision Stat.

Roller

Roller indgår i de forskellige Profiler og består hver især af et sæt rettigheder til forskellige objekter (eksempelvis tabeller eller formularer) i Navision Stat. Roller kan både indgå i profiler og tilknyttes direkte til brugeren, se nedenstående figur 2.



Figur 2.

Sti : Brugeradministration/Opsætning/Roller

Rolle-id	Navn
NS_BACKUP	Sikkerhedskopiering
NS_BANK	Redigering af banktabeller
NS_BASIS	Læseadgang (basis)
NS_BATCH	Afvikling af batchkørsler
NS_BETALING	Redigering af PM-tabeller
NS_BOGHOLDER	Bogholderifunktion
NS_KASSERER	Kassererfunktion
NS_MEDARB_RED	Redigering af medarbejder data
NS_MEDARB_SE	Læsning af Medarbejderdata
NS_OEKONOMI	Økonomifunktion (basis)
NS_OPS_ANLAEG	Opsætning af Anlæg
NS_OPS_BRUGERADM	Opsætning af Brugeradministr.
NS_OPS_CP	Opsætning af Commerce Portal
NS_OPS_CRM	Opsætning af CRM
NS_OPS_FIN	Opsætning af Finans (basis)
NS_OPS_KOEB	Opsætning af Køb
NS_OPS_LAG	Opsætning af Lager
NS_OPS_LOGISTIK	Opsætning af Logistik (ADCS)
NS_OPS_MPS	Opsætning af MPS (Prod./Kap.)
NS_OPS_PERSONALE	Opsætning af Personale
NS_OPS_RES	Opsætning af Ressourcer
NS_OPS_SAG	Opsætning af Sager
NS_OPS_SALG	Opsætning af Salg
NS_OPS_SERVICE	Opsætning af Service
NS_REVISION	Rigsrev. (beskyttet adgang)
NS_SIKKERHED	Redigere brugere og roller
NS_SLS_OPDAT	Opdatering af løndata fra SLS
NS_SLS_SE	Læsning af løndata fra SLS
NS_TEKNIK	Indlæsning af objektrettelser
NS_TIDSREG	Tidsregistrering
SUPER	This role has all permissions.
SUPER (DATA)	Superbruger på data

Ovenfor ses en liste over de standardroller der findes i Navision Stat. I det følgende er kort beskrevet, hvilke rettigheder de enkelte roller har.

Rolle	Beskrivelse
NS_BACKUP	Rollen giver ret til at udlæse en Navision Stat sikkerhedskopi (objekter og data), men ikke til at indlæse en sikkerhedskopi.
NS_BANK	Rollen giver ret til at redigere i banktabeller, såsom bankkontokort-tabellen, bankpost-tabellen og udførelse af bankkontoafstemninger.

NS_BASIS	Rollen giver ret til at se alle tabeller (dog ikke personale-tabeller) og udskrive rapporter, hvor dette ikke medfører en rettelse i den pågældende tabel.
NS_BATCH	Rollen giver rettigheder til at afvikle batchkørsler.
NS_BETALING	Rollen giver rettigheder til at redigere i Payment Management tabeller (eksempelvis oprettelse af betalingsoplysninger).
NS_BOGHOLDER	Rollen giver rettigheder til en række basale bogholderi-funktioner.
NS_KASSERER	Rollen giver rettigheder til en række basale kasserer-funktioner.
NS_MEDARB_RED	Rollen giver rettigheder til at redigere i medarbejder-data.
NS_MEDARB_SE	Rollen giver rettigheder til at se medarbejder-data.
NS_OEKONOMI	Rollen giver rettigheder til at lægge budgetter og indtaste i sags- og ressource-modulerne.
NS_OPS_ANLAEG	Rollen giver rettigheder til at foretage opsætninger i anlægsmodul. Rollen skal som minimum anvendes sammen med NS_BASIS og NS_OPS_FIN.
NS_OPS_BRUGERADM	Rollen giver rettigheder til at foretage opsætninger i brugeradministrationsmodul. Rollen skal som minimum anvendes sammen med NS_BASIS og NS_OPS_FIN.
NS_OPS_CP	Rollen giver rettigheder til at foretage opsætning af Commerce Portal. Rollen skal som minimum anvendes sammen med NS_BASIS og NS_OPS_FIN.
NS_OPS_CRM	Rollen giver rettigheder til at foretage opsætninger i CRM-modul. Rollen skal som minimum anvendes sammen med NS_BASIS og NS_OPS_FIN.
NS_OPS_FIN	Rollen giver rettigheder til at foretage basis-opsætninger i finansmodul. Rollen skal som minimum anvendes sammen med NS_BASIS.
NS_OPS_KOEB	Rollen giver rettigheder til at foretage opsætninger i købsmodul og i DOPEI. Rollen skal som minimum anvendes sammen med NS_BASIS og NS_OPS_FIN.
NS_OPS_LAG	Rollen giver rettigheder til at foretage opsætninger i lagermodul. Rollen skal som minimum anvendes sammen med NS_BASIS og NS_OPS_FIN.
NS_OPS_LOGISTIK	Rollen giver rettigheder til at foretage opsætninger i logistikmodul. Rollen skal som minimum anvendes sammen med NS_BASIS og NS_OPS_FIN.

NS_OPS_MPS	Rollen giver rettigheder til at foretage opsætninger i produktions- og kapacitetsstyringsmodulet. Rollen skal som minimum anvendes sammen med NS_BASIS og NS_OPS_FIN.
NS_OPS_PERSONALE	Rollen giver rettigheder til at foretage opsætninger i personalemodulet. Rollen skal som minimum anvendes sammen med NS_BASIS og NS_OPS_FIN.
NS_OPS_RES	Rollen giver rettigheder til at foretage opsætninger i ressourcemodulet. Rollen skal som minimum anvendes sammen med NS_BASIS og NS_OPS_FIN.
NS_OPS_SAG	Rollen giver rettigheder til at foretage opsætninger i sagsmodulet. Rollen skal som minimum anvendes sammen med NS_BASIS og NS_OPS_FIN.
NS_OPS_SALG	Rollen giver rettigheder til at foretage opsætninger i salgsmodulet. Rollen skal som minimum anvendes sammen med NS_BASIS og NS_OPS_FIN.
NS_OPS_SERVICE	Rollen giver rettigheder til at foretage opsætninger i servicemodulet. Rollen skal som minimum anvendes sammen med NS_BASIS og NS_OPS_FIN.
NS_OPS_PROKURA	Rollen giver rettigheder til at foretage opsætninger af bankprokura, herunder grupper og brugere.
NS_REVISION	Rollen giver se-adgang til alle tabeller (incl. personaletabeller) samt ret til at udskrive alle rapporter. Rollen giver via ret lov til at indsætte rapporter i rapportlisten samt at indlæse objekter af typen dataport og rapporter (der kan ikke foretages ændringer eller sletninger af disse objekttyper).
NS_SIKKERHED	Rollen giver ret til at tildele rettigheder til andre brugere.
NS_SLS_OPDAT	Rollen giver ret til at afvikle kørslen 'Opdater medarbejderoplysninger'.
NS_SLS_SE	Rollen giver rettigheder til at se løn-data.
NS_TEKNIK	Rollen giver ret til at indlæse sikkerhedskopier (kun objekter) og objektfiler (uden data). Bemærk: Såfremt indlæsningen indeholder nye objekter, kræves det, at Navision-brugeren med rollen NS_TEKNIK ligeledes er tildelt dbo-rettigheder på MS SQL-serveren.
NS_TIDSREG	Rollen giver adgang til at registrere i tidsregistreringskladden.
SUPER	Rollen giver rettigheder til at foretage alt i Navision Stat.
SUPER (DATA)	Rollen giver rettigheder til at læse, indsætte, redigere samt slette i alle tabeldata.

Sti : Brugeradministration/Opsætning/Roller/menuknappen
Rolle/menupunktet **Rettigheder**.

O..	Objekt-id	Objektnavn	L...	I...	R...	S...	U..
Tab	17	Finanspost		I..	I..	I..	
T..	21	Debitorpost		I..	I..	I..	
T..	25	Kreditorpost		I..	I..	I..	
T..	32	Varepost		I..	I..	I..	
T..	45	Finansjournal		I..	I..	I..	
T..	46	Varejournal		I..	I..	I..	
T..	50	Regnskabsperiode		Ja	Ja	Ja	
T..	86	Kursregul.journal		I..	I..	Ja	
T..	87	Datokomprim.journal		I..	I..	Ja	
T..	160	Ressourcekapc.post		I..	I..	I..	
T..	169	Sagspost		I..	I..	I..	

På ovenstående skærmbillede ses et udsnit af de rettigheder, som rollen NS_BOGHOLDER indeholder.

Felt navn	Beskrivelse
Objekttype	Feltet indeholder den objekttype, som rettighederne gælder for i den aktuelle database. Følgende valgmuligheder forefindes: <ul style="list-style-type: none"> • Table Data; Tabeldata • Table; Tabel • Form; Formular • Report; Rapport • Dataport; Dataenhed • Codeunit; Kodeenhed • System; System
Objekt-id	Feltet viser id'en for det objekt, som rettighederne gælder.
Objektnavn	Feltet viser navnet på det objekt, som rettighederne gælder.
Læserettighed (Tabel data)	I feltet angives, om rollen har rettigheden til at læse i pågældende tabel. Følgende valgmuligheder forefindes: <ul style="list-style-type: none"> • Ja • Indirekte; har læserettigheder til objektet men via omveje (f.eks. fra andre tabeller). • Blankt <p>Bemærk: Hvis feltet er blankt, har rollen ikke rettigheden til at læse objektet.</p>

Indsæt rettighed (Tabel data)	I feltet angives, om rollen har rettigheden til at indsætte (skrive) i pågældende tabel. Følgende valgmuligheder forefindes: <ul style="list-style-type: none"> • Ja • Indirekte; har indsætterrettigheder til objektet men via omveje (f.eks. via bogføring). • Blankt Bemærk: Hvis feltet er blankt, har rollen ikke rettigheden til at indsætte noget i objektet.
Rediger rettighed (Tabel data)	I feltet angives, om rollen har rettigheden til at rette i pågældende tabel. Følgende valgmuligheder forefindes: <ul style="list-style-type: none"> • Ja • Indirekte; har redigeringsrettigheder til objektet men via omveje (f.eks. markering af udlignings-id). • Blankt Bemærk: Hvis feltet er blankt, har rollen ikke rettigheden til at rette objektet.
Slet rettighed (Tabel data)	I feltet angives, om rollen har rettigheden til at slette i pågældende tabel. Følgende valgmuligheder forefindes: <ul style="list-style-type: none"> • Ja • Indirekte; har sletterrettigheder til objektet men via omveje (f.eks. bogføring, der sletter kladdelinier). • Blankt Bemærk: Hvis feltet er blankt, har rollen ikke rettigheden til at slette objektet.
Udfør rettighed (Codeunits)	I feltet angives, om rollen har rettigheden til at udføre/afvikle den pågældende kode. Følgende valgmuligheder forefindes: <ul style="list-style-type: none"> • Ja • Indirekte; har udførerrettigheder til objektet men via omveje (f.eks. via kørsler). • Blankt Bemærk: Hvis feltet er blankt, har rollen ikke rettigheden til at udføre/afvikle koden.

Betingede rettigheder

Sti: Funktioner/Sikkerhed/Roller/menuknappen Rolle/Rettigheder.

Ønsker du, at gøre rettigheder betinget af indholdet i visse felter, kan du gøre dette på rolleniveau ved at oprette en sikkerhedsfilter på de relevante tabeller. Da sikkerhedsfilter er på rolleniveau, kan det være nødvendigt at oprette nogle lokale roller til formålet.

Ønsker du f.eks. at gøre se adgangen til lønnummer tabellen afhængig af hvilken Administrativt tjenested en medarbejder tilhører og har institutionen 2 forskellige administrative tjenestesteder (1A og 2A), skal der oprettes 2 nye roller (ABC_MEDARB_SE_1A og ABC_MEDARB_SE_2A), som begge tildeles rettigheder svarende til NS_MEDARB_SE.

Herefter åbnes ABC_MEDARB_SE_1A's rettighedsvindue:

Objekttype	Objekt-id	Objektnavn	Læ...	I...	Re...	U..	Sikkerhedsfilter
Table Data	5200	Lønnummer	Ja				...
Table Data	5201	Alternativ adresse	Ja				
Table Data	5202	Kvalifikation	Ja				
Table Data	5203	Medarbejderkvalifikation	Ja				
Table Data	5204	Familiemedlem	Ja				
Table Data	5205	Medarbejders familiemedl...	Ja				
Table Data	5206	Fraværsårsag	Ja				
Table Data	5207	Medarbejders fravær	Ja				
Table Data	5208	Medarbejderbemærkning	Ja				
Table Data	5209	Fagforening	Ja				
Table Data	5210	Inaktivitetsårsag	Ja				

Buttons: Alle objekter, Hjælp

Find den relevante tabel (5200) og tryk på ... i feltet Sikkerhedsfilter. Herefter åbnes tabelfilter vinduet, som udfyldes som nedenstående:

Felt	Filter
Adm. tjenestested	1A
*▶	

Buttons: OK, Annuller, Anvend, Hjælp

Herefter har brugere, som har rollen ABC_MEDARB_SE_1A kun adgang til at se lønnumre med Adm. Tjenestested 1A. Tilsvarende gøres for rollen ABC_MEDARB_SE_2A.

Nedenstående eksempel illustrerer sammenhængen mellem profiler og roller.

Rolle-id	Navn	OES_BOGH...	OES_FBOGH...	OES_FKASS...	OES_FPERS...	OES_FSLIS...	OES_KASSE...
N5_BACKUP	Sikkerhedskopiering						
N5_BANK	Redigering af banktabeller	Ja	Ja	Ja			Ja
N5_BASIS	Læseadgang (basis)	Ja	Ja	Ja	Ja	Ja	Ja
N5_BATCH	Afvikling af batchkørsler						
N5_BETALING	Redigering af PM-tabeller	Ja	Ja				
N5_BOGHOLDER	Bogholderfunktion						
N5_KASSERER	Kasserefunktion			Ja			Ja
N5_OEKONOMI	Økonomifunktion (basis)	Ja	Ja	Ja			Ja
N5_OPS_ANLAEG	Opsætning af Anlæg						
N5_OPS_BRUGERADM	Opsætning af Brugeradministr.						
N5_OPS_CP	Opsætning af Commerce Portal						
N5_OPS_CRM	Opsætning af CRM						
N5_OPS_FIN	Opsætning af Finans (basis)						
N5_OPS_KOEB	Opsætning af Køb						
N5_OPS_LAG	Opsætning af Lager						
N5_OPS_LOGISTIK	Opsætning af Logistik (ADCS)						
N5_OPS_MPS	Opsætning af MPS (Prod./Kap.)						
N5_OPS_PERSONALE	Opsætning af Personale						
N5_OPS_RES	Opsætning af Ressourcer						
N5_OPS_SAG	Opsætning af Sager						
N5_OPS_SALG	Opsætning af Salg						
N5_OPS_SERVICE	Opsætning af Service						
N5_PERSONALE_RED	Redigering af Personaledata					Ja	

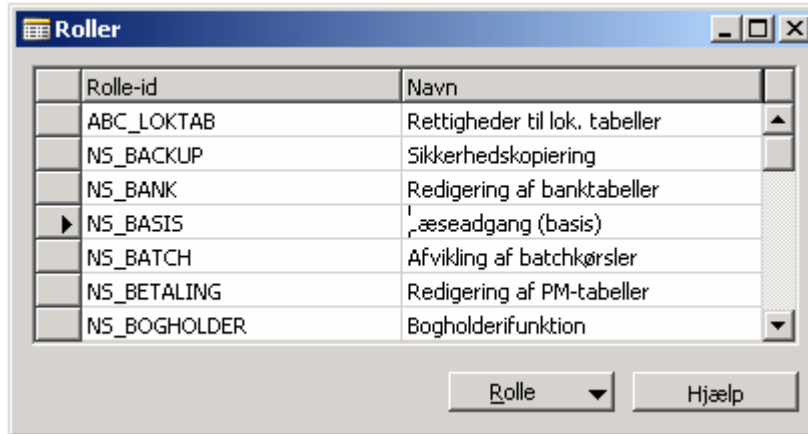
Brugere kan både få tildelt roller og profiler. Fordelen ved at tildele profiler er, at man ikke skal tildele så mange roller til de enkelte brugere. Desuden giver det et bedre overblik over hvilken type medarbejder, de forskellige brugere er.

Profilerne kan laves, så de afspejler institutionens struktur og arbejdsgange. Sammensætningen af Profilerne skal altid ske i overensstemmelse med sikkerhedsinstruksen. For yderligere retningslinjer for sammensætning af lokale profiler se afsnittet ”Best Practise”.

Eksempel på oprettelse af ny Rolle

Sti : Brugeradministration/Opsætning/Brugeradministrationsopsætning/Rolle.
 Institution ABC har fået lavet 2 lokale tabeller (tabel 50000 og 50050) og har brug for en rolle, som giver hhv. alle rettigheder til tabel 50000 og læserettighed til tabel 50050.

1. Vælg Brugeradministration/Opsætning/Roller.
2. Udfyld felterne Rolle-ID og Navn. Du bør lade institutionens navn indgå i navnet på Rolle-ID (ABC_XXXX), således at de let adskiller sig fra Økonomistyrelsens roller. For uddybende begrundelse se afsnittet ” Best Practise”.



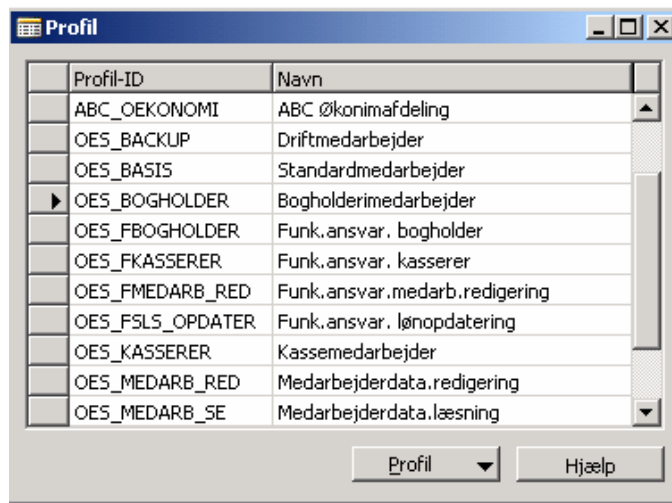
3. For at tilknytte rettigheder til roller skal du trykke på menuknappen **Rolle** og vælge **Rettigheder**. For at opnå de ovenfor nævnte rettigheder som rettighedstabellen udfyldes som nedenstående:

Objekttype	Objekt-id	Objektnavn	Læs...	Inds...	Redige...	Slet...	Udfør ...
Table Data	50000	Lokal tabel 1	Ja	Ja	Ja	Ja	Ja
Table Data	50050	Lokal tabel 2	Ja				

Eksempel på oprettelse af ny Profil

Sti : Brugeradministration/Opsætning/Brugeradministrationsopsætning/Profil
 Institution ABC ønsker, at tildele alle økonomimedarbejdere en profil (ABC_OEKONOMI), som svarer til OES_OEKONOMI, dog med tilføjelse af rollerne ABC_LOKTAB og NS_OPS_FIN
 Følg nedenstående trin for at lave profilen ABC_OEKONOMI

1. Vælg Brugeradministration/Opsætning/Profiler
2. Udfyld felterne Profil-ID og Navn med henholdsvis ABC_OEKONOMI og et sigende navn, f.eks. Økonomiafd. ABC.



Ved at navngive profilerne med institutionens navn (ABC_) er det let at adskille de lokale profiler fra Økonomistyrelsens profiler. I stedet for at udvide profilerne fra Økonomistyrelsen bør man lave sine egne profiler med udgangspunkt i profilerne fra Økonomistyrelsen. For uddybende begrundelse se afsnittet ” Best Practise”.

Bemærk: Under fanebladet Generelt/vinduet Brugeradministrationsopsætning kan du angive, om du ønsker automatisk at overføre profiler til SQL-serveren. Såfremt du har valgt automatisk at overføre profiler, vil der ved oprettelse af en profil i Navision blive oprettet en database-rolle på SQL-serveren med samme navn. Har du ikke valgt automatisk overførelse, skal du køre den periodiske aktivitet ”Overfør profiler” (Sti : Brugeradministration/Periodiske aktiviteter/Overfør profiler).

På SQL-serveren vil der nu være oprettet en database-rolle (denne må ikke forveksles med Navisions rollebegreb) kaldet ABC_OEKONOMI. Rollen har endnu ingen rettigheder.

3. For at knytte Navision-roller til en profil skal du i vinduet Profiler vælge menuknappen **Profil**/menupunktet **Roller**. Til profilen ABC_OEKONOMI skal du knytte følgende roller:

Rolle-ID	Navn
ABC_LOKTAB	Rettigheder til lok. tabeller
NS_BASIS	Læseadgang (basis)
NS_OEKONOMI	Økonomifunktion (basis)
NS_OPS_FIN	Opsætning af Finans (basis)
*▶	↑

På SQL-serveren kan man nu se, at database-rolle ABC_OEKONOMI har fået tildelt select-rettigheder (læseadgang) til netop de tabeller, som Økonomistyrelsens roller NS_BASIS, NS_OEKONOMI og NS_OPS_FIN og ABC rolle ABC_LOKTAB har læse-rettighed til.

Bemærk: Kun NS_BASIS har læseadgang – de andre roller har skrive/rette/slette adgang.

Indlæsning af rettigheder og roller

Økonomistyrelsen har et sæt standardroller og –rettigheder, som institutionen frit kan tilknytte deres medarbejdere. Disse indarbejdes i en tekstfil, som i nogle tilfælde opdateres sammen med frigivelse af objektændringer i Navision Stat. Der kan i den forbindelse være behov for rettighedstildeling til nye objekter eller ændret rettighedstildeling til eksisterende objekter. Dette bør dog aldrig gøres i selve standardprofiler- eller roller, men i en lokal kopi. For uddybende begrundelse se afsnittet ” Best Practise”.

Indlæsningen af rettigheder og roller foregår via periodiske aktiviteter.
Sti: Finans/Periodiske aktiviteter/Kombineret rettighedsind-/udlæsning



Bemærk: Ved afvikling af denne kørsel sker der følgende:

- Enten overskrives eksisterende roller og rettigheder.
- Eller nye roller og rettigheder tilføjes.

Indlæsning vil aldrig medføre en sletning af rettigheder. Dette må enten ske manuelt eller via datakonvertering i forbindelse med en indlæsning af en objektopdatering via det lokale versionsstyringsystem VMS (for yderligere beskrivelse se manual vedr. VMS menuen). I sidstnævnte tilfælde styres sletningen af Økonomistyrelsen.

Kørslen kan bruges til både ud- og indlæsning af tekstfilen.

Hvem kan oprette brugere ?

Når der skal oprettes brugere i Navision Stat, skal du være opmærksom på, at ikke alle brugere i Navision Stat har rettigheder dertil. Som det efterfølgende bliver nævnt i afsnittet, er det kun superbrugeren i Navision Stat samt de funktionsansvarlige brugere, der kan oprette nye brugere og redigere i eksisterende brugeres rettigheder.

Superbruger

På SQL-serveren oprettes superbrugeren som dbo (database owner) på databasen og tildeles serverrollen Security Administrator. Dermed kan denne udføre samtlige opgaver i Navision Stat og har alle nødvendige rettigheder på SQL-serveren.

Det er også for det meste med denne superbruger, man opretter nye brugere eller redigerer i eksisterende brugeres rettigheder.

Den første bruger, der oprettes i Navision Stat, er altid superbrugeren, der skal have tildelt rollen Super, som har alle rettigheder.

Funktionsansvarlige brugere

Udover superbrugeren har brugerne med funktionsansvarlige profiler også rettigheder til at oprette brugere. Disse brugere kan dog blot tildele de nye brugere rettigheder, der maksimalt svarer til deres egne. F.eks. kan en funktionsansvarlig kasserer oprette en ny bruger og tildele denne bruger til og med kasserer-rettigheder.

I Navision Stat findes der 4 typer funktionsansvarlige profiler,

OES_FBOGHOLDER
OES_FKASSERER
OES_FMEDARB_RED
OES_FSLS_OPDATER

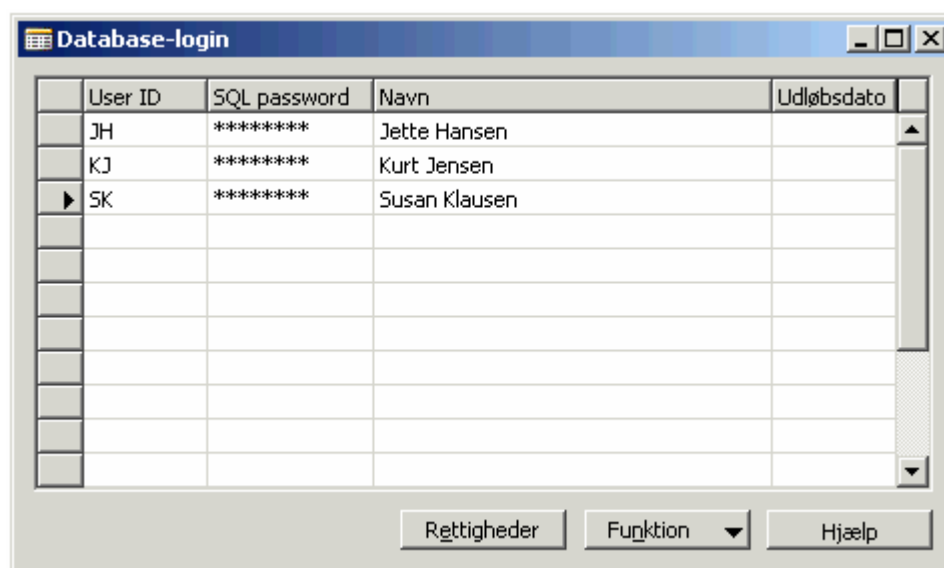
Alle 4 profiler indeholder rollen NS_SIKKERHED, der giver adgang til tildeling af rettigheder til andre brugere.

Brugeroprettelse

Når der skal oprettes brugere i Navision Stat, kan disse enten oprettes som Windows-logins eller Databaselogins. I det følgende gennemgås de to muligheder.

Databaselogin

Sti : Brugeradministration/Databaselogin



Bemærk: Når brugeren bliver oprettet som databaselogin, skal der indtastes adgangskode, når brugerne logger på Navision-databasen.

Felt navn	Beskrivelse
User ID	Her skal du indtaste brugerens bruger-id.
SQL password	Her skal du angive et password for den pågældende bruger. Hvis du ikke indtaster nogen værdi i feltet, vil password være blank for den pågældende bruger, når denne logger sig på databasen. Bemærk: I tilfælde af at brugeren er oprettet i en anden database med et andet password (og brugeren dermed allerede eksisterer på SQL-serveren), vil det være brugerens allerede eksisterende password der er gældende.
Navn	Her skal du indtaste brugerens navn.
Udløbsdato	Her kan du indtaste den dato, efter hvilken brugeren ikke længere vil kunne logge sig på den pågældende database. Bemærk: SUPER-brugeren må ALDRIG oprettes med udløbsdato.

Eksempel

Dette eksempel tager udgangspunkt i, at brugeren 'Birgit Jensen' skal oprettes som databaselogin 'BJ' i Navision Stat 3.60.

For at oprette databaselogin'et skal nedenstående trin følges,

1. Vælg Brugeradministration/Databaselogin
2. Udfyld vinduet 'Databaselogin' med
Bruger-ID : *BJ*
SQL-password : *123456*
Navn : *Birgit Jensen*
Udløbsdato : *31-12-05*

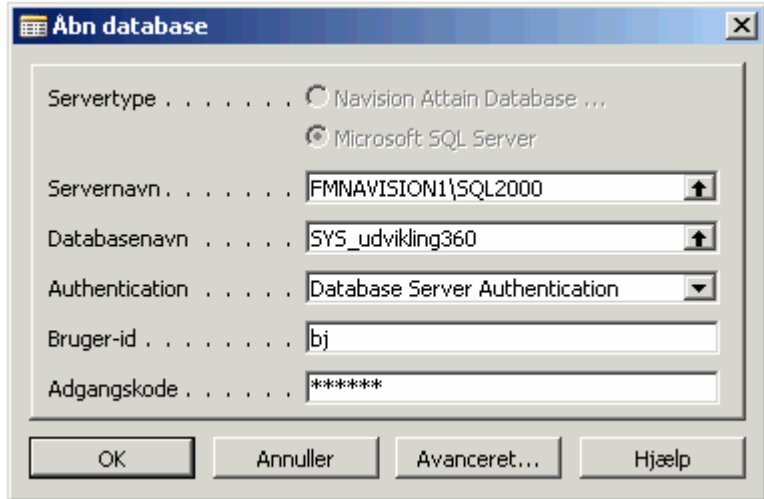
Når feltet SQL-password udfyldes, gemmes password i Navision Stat-databasen. Vær opmærksom på, at feltet er case-sensitiv (checker på store og små bogstaver).



3. Når brugeren er oprettet, tildeles brugeren rettigheder ved at markere brugeren og vælge knappen "Rettigheder". Herefter kan brugeren tildeles den ønskede profil.
-



På SQL-serveren er brugeren 'BJ' nu blevet oprettet.
Når brugeren efterfølgende logger sig på databasen vha
Filer/Database/"Åbn...", skal skærmbilledet se ud som vist nedenstående.



Windowslogin

Sti : Brugeradministration/Windows-login

Når brugeren bliver oprettet som Windowslogin, skal brugeren inden da være oprettet på institutionens netværk. Det kræver ingen adgangskode at logge på Navision Stat-databasen, fordi valideringen af bruger-ID og password allerede er sket, da brugeren loggede sig på institutions-netværket.

Når der oprettes windowslogin skal den oprettende bruger have serverrolen Security administrator. Ved oprettelse af windowslogin er det således ikke tilstrækkeligt at forbindelsesbrugeren har visse serverrettigheder.

Bemærk: Når man logger på basen skal "Windows authentication" være valgt i vinduet "Åbn database".

Windowslogin kræver, at filen xp_ndo.dll er installeret på serveren.

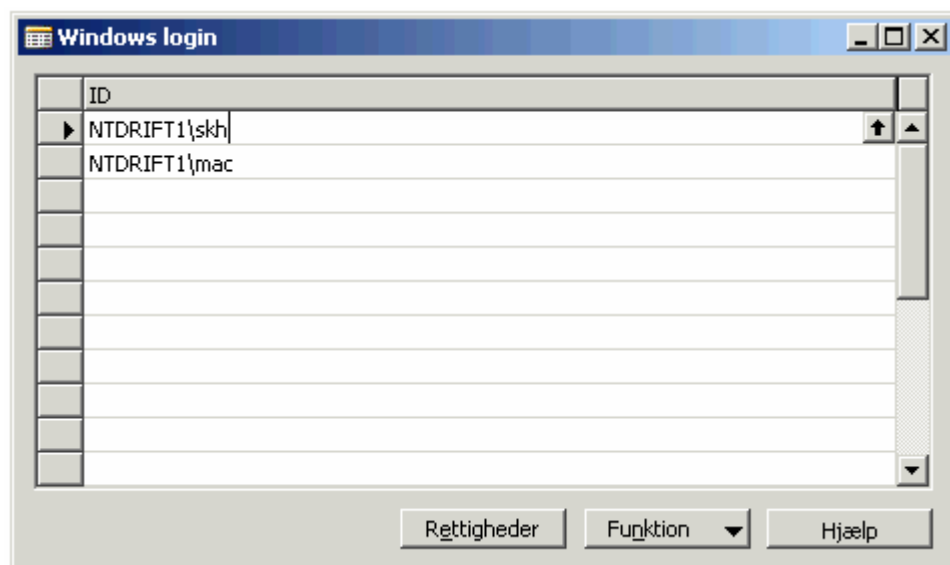
For at oprette Windowslogin skal klienten anvende operativsystemet Windows 98, Windows 2000 eller Windows XP.

Eksempel

Dette eksempel tager udgangspunkt i, at brugeren "skh" skal oprettes som windowslogin i Navision Stat. Brugeren er allerede oprettet på domænet "NTDRIFT1".

For at oprette et windowslogin skal nedenstående trin følges:

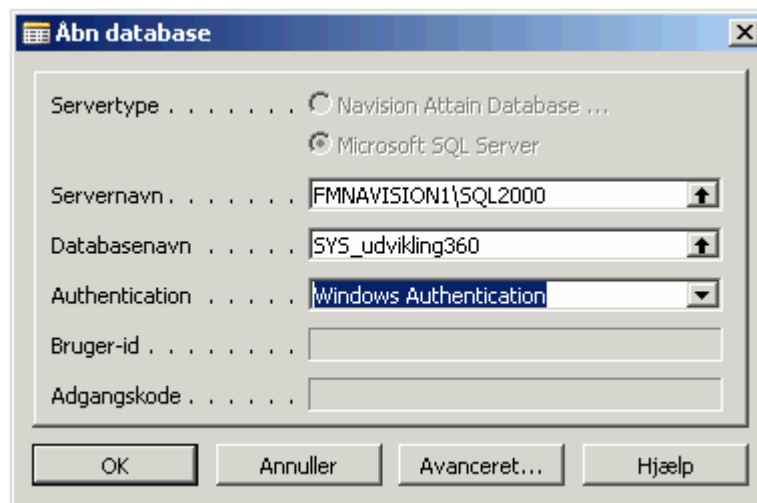
- Vælg Brugeradministration/Windows-login
- Udfyld vinduet Windows-login med Bruger-ID "skh".



Brugeren oprettes med samme initialer/bruger-ID, som vedkommende er oprettet med på netværket. Notationen er Domæne\Bruger-ID, hvor Domæne er det netværksdomæne, brugeren anvender, og Bruger-ID er brugerens login-navn på domænet.

Bemærk: Det er ikke nødvendigt at indtaste domænenavnet, da systemet selv kan håndtere dette. Dvs at linien blot udfyldes med initialerne 'skh'.

- Når brugeren er oprettet, tildeles brugeren rettigheder som ved databaselogin. Klik på knappen **Rettigheder** og tildel brugeren den ønskede profil.
- Når brugeren efterfølgende logger sig på databasen vha Filer/Database/'Åbn...', skal skærmbilledet se ud som vist nedenfor.



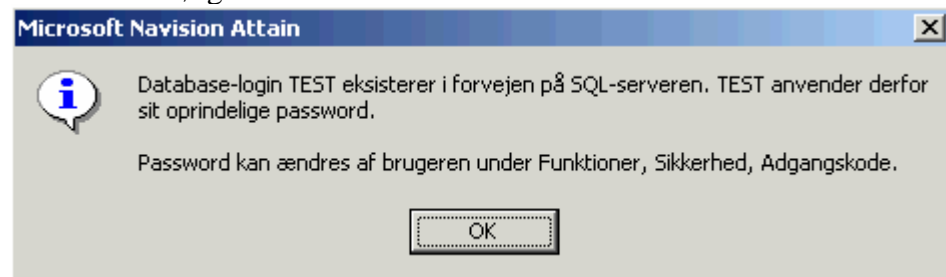
Validering

I forbindelse med oprettelse af databaselogin, bliver værdien i feltet "SQL-password" gemt i Navision Stat-databasen. Der skal endvidere gøres opmærksom på, at der efter indtastning af password sker en validering af feltværdien. I tilfælde af at brugeren allerede er oprettet i en anden database på samme SQL-server med et givent password, vil systemet gøre opmærksom på dette, hvis samme bruger forsøges oprettet med et andet password.

Eksempel

Dette eksempel tager udgangspunkt i at brugeren TEST er oprettet i en anden database (på SQL-serveren 'FMNAVISION\SQL2000') med password 12345678. Det forsøges nu at oprette samme bruger i 'SYS-udvikling360'-databasen (på SQL-serveren 'FMNAVISION\SQL2000') med password 87654321.

Herefter fås følgende meddelelse:



Kopiering af rettigheder

Når brugeren oprettes som Database-login eller Windows-login, tildeles denne efterfølgende et sæt rettigheder. Den måde, at tildele rettigheder på, kaldes den manuelle metode.

Det er også muligt at kopiere rettigheder fra en bruger til en anden. Dette er særlig anvendeligt i de tilfælde, hvor man allerede har oprettet en bruger med forskellige rettigheder, og der efterfølgende skal oprettes en række nye brugere med de samme funktioner (rettigheder) i Navision Stat. Det kan forenkle processen, hvis rettighederne kopieres fra den allerede eksisterende bruger til den nye, i stedet for at der manuelt tildeles rettigheder til hver af de nye brugere.

Eksempel på kopiering af rettigheder

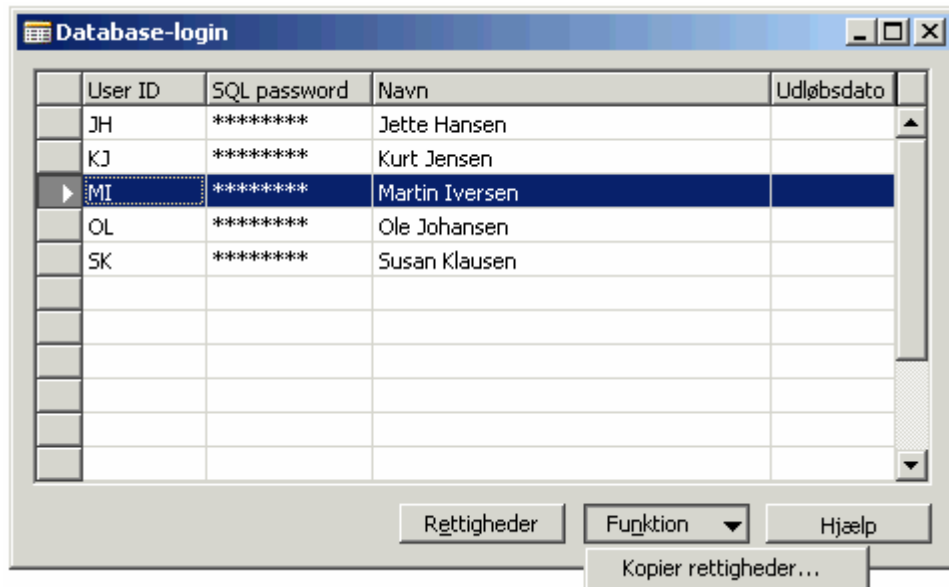
I eksemplet tages udgangspunkt i brugeren Ole Johansen med bruger-id OL, der har fået tildelt følgende rettigheder i Navision Stat:



Type	ID	Navn
Profil	OES_BOGHOLDER	Bogholderimedarbejder
Rolle	NS_BATCH	Afvikling af batchkørsler
Rolle	NS_OPS_FIN	Opsætning af Finans (basis)
Rolle	NS_OPS_KOEB	Opsætning af Køb

Der skal nu oprettes en ny bruger Martin Iversen, der skal have de samme rettigheder som Ole Johansen.

Den nye bruger bliver oprettet i vinduet 'Database-login' med bruger-ID *MI*, SQL password er *<blankt>* og bruger-navn *Martin Iversen*.



Herefter tildeles Martin Iversen rettigheder ved at anvende funktionen 'Kopier rettigheder'.



I det fremkomne skærbillede angives fra hvilken bruger, der skal kopieres og til hvilken bruger, der skal kopieres. I dette tilfælde fra bruger Ole Johansen med bruger-ID OL til bruger Martin Iversen med bruger-ID MI.

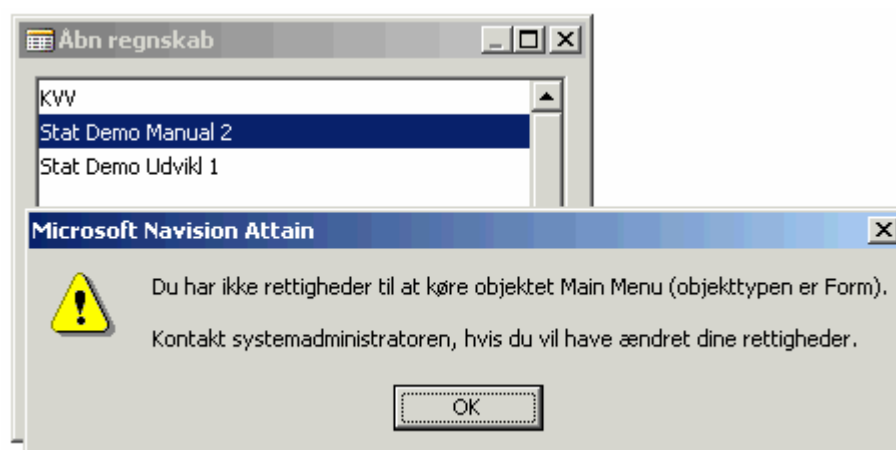
Fejlbeskeder samt årsag

I dette afsnit er der beskrevet nogle af de fejlbeskeder, man som brugeradministrator kan komme ud for.

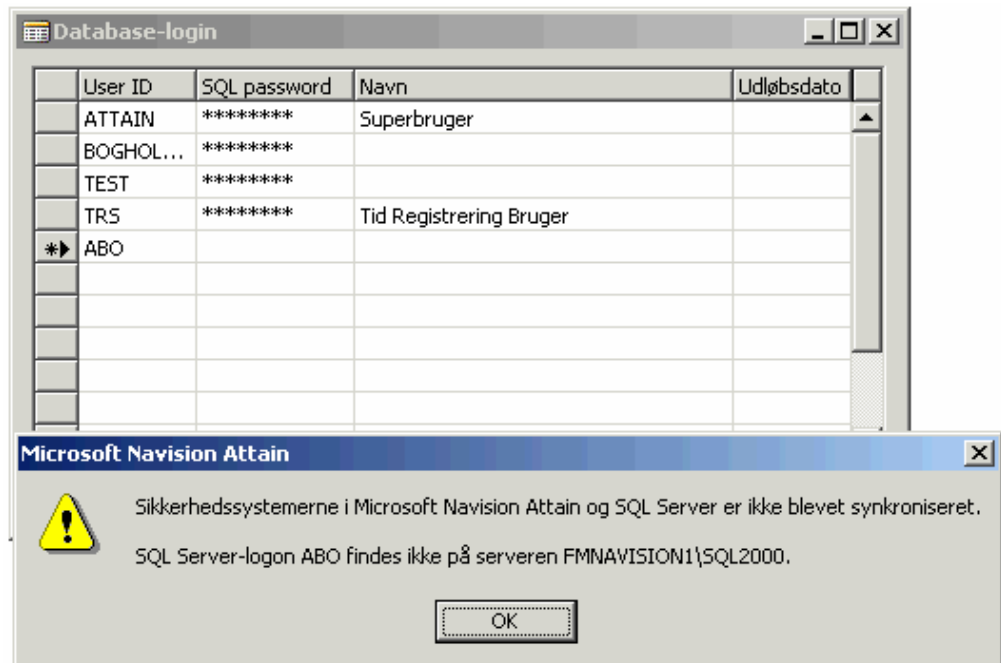
Ej overførsel af brugerlogin til sql-server

Hvis der i brugeradministrationsopsætningen ikke er opsat, at der skal overføres databaselogin til SQL-serveren, skal du manuelt ved hjælp af periodiske aktiviteter sørge for at overføre login til serveren.

Hvis dette ikke foretages, vil brugeren få en fejlmeddelelse, når denne forsøger at logge sig på databasen.

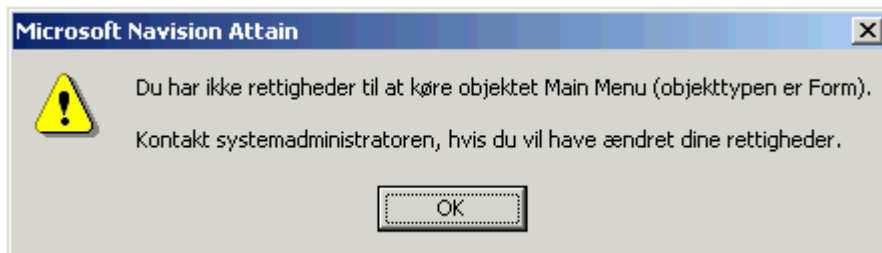


I enkelte tilfælde kan brugeradministratoren også komme ud for følgende fejlbesked, hvis der ikke er opsat, at databaselogin skal overføres til SQL-serveren.



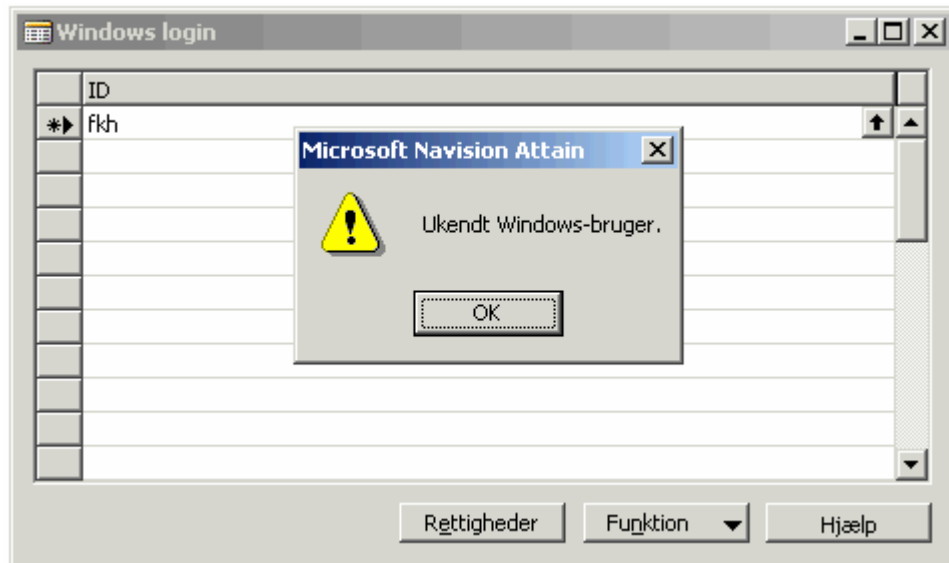
Ej tildeling af rettigheder til brugeren

Det kan ske, at der bliver oprettet en bruger, men at man glemmer at tildele brugeren rettigheder. Hvis dette sker, vil brugeren få en fejlmeddelelse om, at vedkommende ikke har rettigheder til "en bestemt tabel".



Brugeren er ikke oprettet på netværket

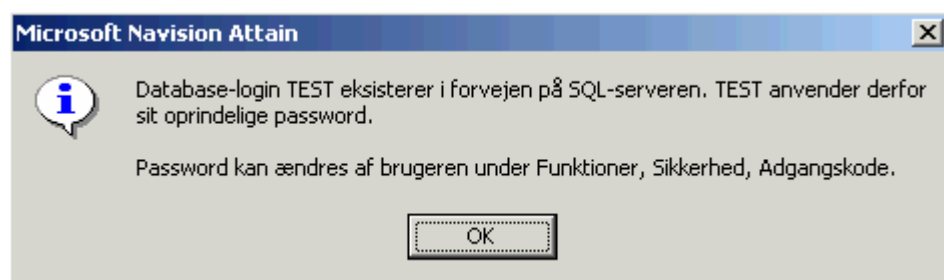
Hvis brugeren skal oprettes som windowslogin i Navision Stat, og denne ikke forinden er blevet oprettet på institutionens netværk, vil brugeradministratoren få følgende fejlbesked:



Brugeren er oprettet i en anden database med et andet password

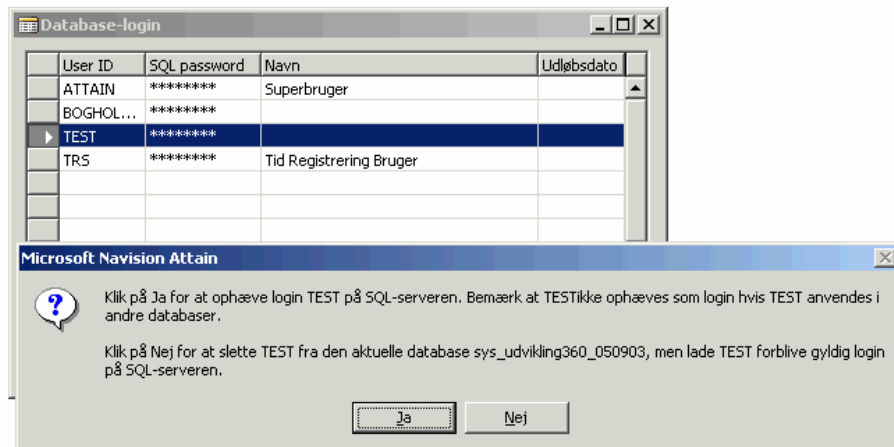
I tidligere Navision Stat-versioner har det været således, at selvom en bruger var oprettet i en database med et givent password, så kunne denne bruger oprettes i en anden database, hvor der i feltet SQL-password kunne indtastes et andet password. Brugeradministratoren troede dermed, at brugeren nu var oprettet i 2 forskellige databaser med 2 forskellige passwords, selvom det rent faktisk er det første password, der er gældende for brugeren i databaser, denne er oprettet i.

I Navision Stat 3.60 sker der en validering i feltet SQL-password. Hvis brugeren forsøges oprettet i en anden database med et nyt password, vil systemet komme op med følgende meddelelse:



Sletning af en Navision Stat bruger

Hvis en bruger skal slettes fra en Navision Stat-database, markeres brugeren, og der trykkes **F4** eller **Delete**. Herefter fås følgende meddelelse:



Hvis der vælges Ja og brugeren ikke anvendes i andre baser slettes denne både på databasen og på SQL-serveren. Hvis brugeren anvendes i andre databaser på serveren slettes brugeren på databasen, men forbliver gyldigt login på serveren.

Vælges Nej, slettes brugeren kun som bruger i den aktuelle database. Brugerens login forbliver således gyldigt på SQL-serveren

Omdøbning af en bruger

I tilfælde af at der opstår et behov for at omdøbe et eksisterende Navision login, kan det foretages på følgende vis:

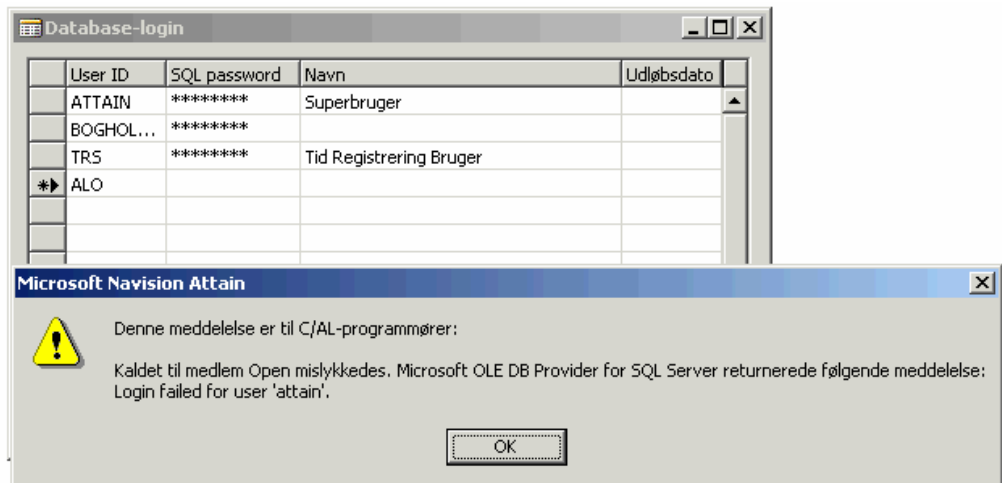
- Opret det nye login
- Kopier rettighederne fra det login, der ønskedes omdøbt, til det nye login
- Slet det login, der ønskedes omdøbt

Følges ovenstående procedure ikke, men forsøges det i stedet at omdøbe det gamle login, vil du få følgende meddelelse:



Ændring af superbrugers password

Når superbrugers password ændres i Navision Stat-databasen, bliver ændringen også foretaget i vinduet Brugeradministrationsopsætning/Faneblad Forbindelse og feltet "Password". Dette bevirker at følgende fejl ved ny brugeroprettelse **undgås**:



Bemærk: 'attain' er superbruger i denne Navision Stat-database.

Ændring af password i Navision Stat

Database login Den adgangskode, der tildeles ved brugeroprettelse, er foreløbig og bør ændres af den enkelte bruger ved første login. Endvidere bør der i overensstemmelse med sikkerhedsinstrukset blive foretaget et password udskift mindst hver 3. måned eller tidligere i tilfælde af, at det er kommet til andres kendskab.

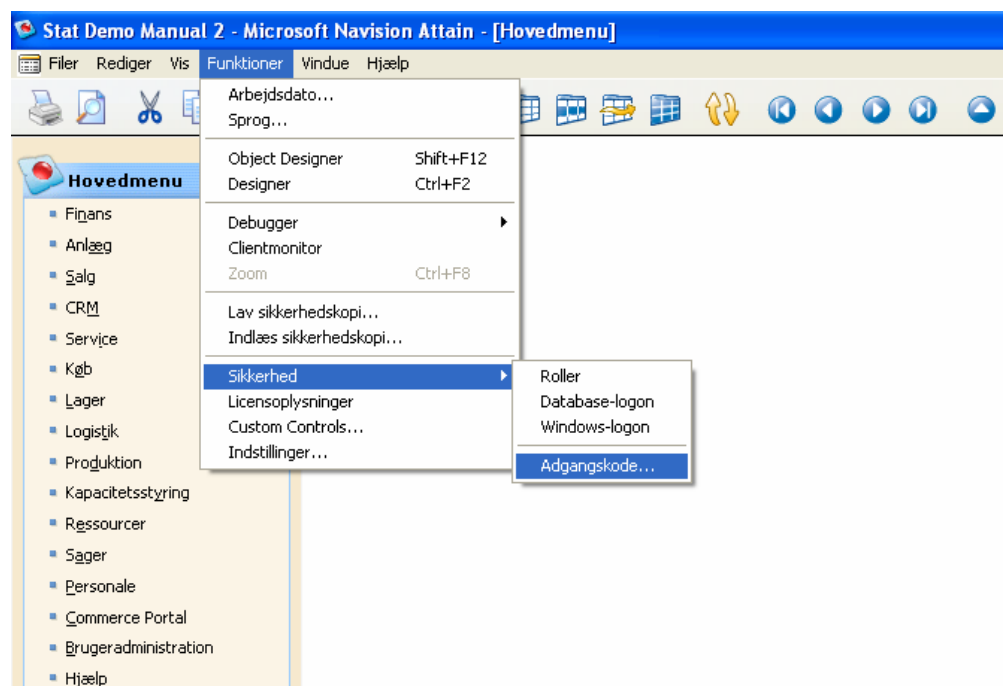
Windows login I forbindelse med windows login tildeles brugeren ikke noget password i Navision Stat, da brugeren i dette tilfælde anvender det password som brugeren er tildelt under oprettelse på institutionens netværk. Derfor skal brugeren ikke ændre password i Navision Stat, men bliver efter en bestemt periode bedt om at skifte sin adgangskode, når denne logger sig på netværket.

Bemærk: Økonomistyrelsen anbefaler, at der anvendes Windows authentication for alle brugere på nær SUPER-brugeren, der typisk er en funktion ved siden af brugerens normale funktion i det daglige.

Ændring af password

Selve ændring af password foretages ved at brugeren logger sig på med det nuværende password.

I dette eksempel tages udgangspunkt i brugeren Jette Hansen. Herefter vælges Funktioner/Sikkerhed/Adgangskode som vist på nedenstående.



Herefter fås følgende vindue:



Her indtastes den nuværende adgangskode, den nye adgangskode og til sidst bekræftes den nye adgangskode.

Felt navn	Beskrivelse
Bruger-id	Her ses bruger-id for den bruger, der er logget på databasen. Der kan ikke redigeres i feltet.
Brugernavn	Her ses brugernavn for den bruger, der er logget på databasen. Der kan ikke redigeres i feltet.
Nuværende adgangskode	Her skal du indtaste din nuværende adgangskode.
Ny adgangskode	Her skal du indtaste den nye adgangskode.
Skriv adgangskode igen	Her skal du indtaste den nye adgangskode igen, og dermed bekræfte den nye adgangskode.

Rapportering

De rapportudskrifter, der er tilgængelige i brugeradministrationsmodulet i Navision Stat 3.60, gennemgås nedenfor. Rapporterne er oplistet med en indholdsbeskrivelse samt et udsnit af rapportudskrifterne.

Brugerliste

Rapporten viser en liste over alle oprettede brugere, der har adgang til programmet. Rapporten viser bruger-ID, navn, dato indtil hvilken bruger-ID'et er gyldigt samt rolle/profil.

User ID	Navn	Udløbsdato	Type	ID	Navn	Regnskab
1			Rolle	NS_BANK		
			Rolle	NS_BASIS		
			Rolle	NS_BETALING		
			Rolle	NS_BOGHOLD		
			Rolle	NS_OEKONOMI		
ATTAIN	Superbruger		Profil	OES_FKASSER	Funk.ansvar. kassener	
			Rolle	SUPER	This role has all permissions	
JH	Jette Hansen		Profil	OES_BOGHOL	Bogholdermedarbejder	
			Rolle	NS_OPS_FIN	Opsætning af Finans (basis)	
			Rolle	NS_OPS_KOEB	Opsætning af Køb	
			Rolle	NS_OPS_SALG	Opsætning af Salg	
KJ	Kurt Jensen		Profil	OES_TIDSREG	Standardmedarbejder.tidreg.	
MI	Martin Iversen					
OL	Ole Johansen					

Roller pr. bruger

Denne rapport viser en liste over, hvilke roller brugerne er tildelt.

Brugeres rettigheder i Navision Stat			
Stat Demo Manual 2		5. september 2003	
		Side	1
		attain	
Medlem af: Bruger-id: JHIKJ			
Database-login			
Brugernavn: JH			
Navn:	Jette Hansen		
Rolle-id	Rollenavn	Virksomhed	
NS_BANK	Redigering af banktabeller		
NS_BASIS	Læseadgang (basis)		
NS_BETALING	Redigering af PMtabeller		
NS_OEKONOMI	Økonomifunktion (basis)		
NS_OPS_FIN	Opsætning af Finans (basis)		
NS_OPS_KOEB	Opsætning af Køb		
NS_OPS_SALG	Opsætning af Salg		
Brugernavn: KJ			
Navn:	Kurt Jensen		
Rolle-id	Rollenavn	Virksomhed	
NS_BASIS	Læseadgang (basis)		
NS_TIDSREG	Tidsregistrering		
Windows-login			
Login-ID	NTDRIFT\skh		
Rolle-id	SUPER	Virksomhedsnavn	Rollenavn
			This role has all permissions.
Login-ID	NTDRIFT\mac		
Rolle-id	SUPER	Virksomhedsnavn	Rollenavn
			This role has all permissions.

Rettigheder pr. Rettighedsgrp.

Denne rapport viser en liste over alle oprettede brugerroller, der har adgang til programmet. Rapporten viser pr. rolle den enkelte rolles rettigheder i Navision Stat.

Rettigheder pr. rettighedsgruppe			
Stat Demo Manual 2		15. oktober 2003	
		Side	1
		attain	
Rettighed: Rolle-id: NS_BASIS			
Gruppe-ID: NS_BASIS			
Gruppenavn: Læseadgang (basis)			
Objekttype	Objekt-ID	Objektnavn	Læse
Table Data	3	Betalingsbetingelser	Ja
Table Data	4	Værluta	Ja
Table Data	5	Rentebetingelser	Ja
Table Data	6	Debitorprisgruppe	Ja
Table Data	7	Tekst	Ja
Table Data	8	Sprog	Ja
Table Data	9	Land	Ja
Table Data	10	Leveringsform	Ja
Table Data	13	Sælger/indkøber	Ja
Table Data	14	Lokation	Ja
Table Data	15	Finanskonto	Ja
Table Data	17	Finanspost	Ja
Table Data	18	Debitor	Ja
Table Data	19	Deb./fakturarakat	Ja
Table Data	21	Debitorpost	Ja
Table Data	23	Kreditor	Ja
Table Data	24	Kred./fakturarakat	Ja
Table Data	26	Kreditorpost	Ja
Table Data	27	Vare	Ja
Table Data	30	Varetekst	Ja
Table Data	32	Varepost	Ja
Table Data	36	Salgshoved	Ja

Roller pr. profil

Rapporten viser en liste over hvilke roller, de forskellige profiler består af.

Roler pr. profil		21. august 2003	
Stat Demo Manual 2		Side	1
		attain	
Profil-ID	Navn	Rolle-ID	Navn
OES_BACKU	Driftmedarbejder	NS_BACKUP NS_BASIS	Sikkerhedskopiering Læseadgang (basis)
OES_BASIS	Standardmedarbejder	NS_BASIS	Læseadgang (basis)
OES_BOGH	Bogholdermedarbejder	NS_BANK NS_BASIS NS_BETALIN NS_OEKON	Redigering af banktabeller Læseadgang (basis) Redigering af PMtabeller Økonomifunktion (basis)
OES_FB000	Funk.ansvar. bogholder	NS_BANK NS_BASIS NS_BETALIN NS_OEKON NS_SIKKER	Redigering af banktabeller Læseadgang (basis) Redigering af PMtabeller Økonomifunktion (basis) Redigere brugere og roller
OES_FKASS	Funk.ansvar. kasserer	NS_BANK NS_BASIS NS_KASSER NS_OEKON NS_SIKKER	Redigering af banktabeller Læseadgang (basis) Kassererfunktion Økonomifunktion (basis) Redigere brugere og roller

Brugere pr. rolle

Denne rapport viser hvilke brugere, der er knyttet til en given rolle.

Brugere pr. rolle		21. august 2003	
Stat Demo Manual 2		Side	1
		attain	
Rolle-ID	Navn	Bruger-ID	Brugernavn
NS_BANK	Redigering af banktabeller	OES_BOGHOLDER OES_KASSERER	Test af OES_BOGHOLDER Test af OES_KASSERER
NS_BASIS	Læseadgang (basis)	OES_BASIS OES_BOGHOLDER OES_KASSERER	Test af OES_BASIS Test af OES_BOGHOLDER Test af OES_KASSERER
NS_BETALIN	Redigering af PMtabeller	OES_BOGHOLDER	Test af OES_BOGHOLDER
NS_BOGHOL	Bogholderfunktion	OES_BOGHOLDER	Test af OES_BOGHOLDER
NS_KASSER	Kassererfunktion	OES_KASSERER	Test af OES_KASSERER
NS_OEKON	Økonomifunktion (basis)	OES_BOGHOLDER OES_KASSERER	Test af OES_BOGHOLDER Test af OES_KASSERER
SUPER	This role has all permissions.	ATTAIN NTDRIFT1\ekh NTDRIFT1\mac	Superbruger

Brugere pr. objekt

Rapporten viser hvilke brugere, der har adgang til et givent objekt.

Brugere pr. objekt

Stat Demo Manual 2

21. august 2003

Side 1

attain

Objekt: Regnskabsnavn: Stat Demo Manual 2

Database-login:

Regnskabsnavn	Type	ID	Navn	Bruger-ID	Brugernavn
Stat Demo Manual 2	TableData	3	Payment Terms	OES_BASIS	Test af OES_BASIS
				OES_BOGH	Test af OES_BOGHOLDER
				OES_KASSE	Test af OES_KASSERER
Stat Demo Manual 2	TableData	4	Currency	OES_BASIS	Test af OES_BASIS
				OES_BOGH	Test af OES_BOGHOLDER
				OES_KASSE	Test af OES_KASSERER
Stat Demo Manual 2	TableData	5	Finance Charge Terms	OES_BASIS	Test af OES_BASIS
				OES_BOGH	Test af OES_BOGHOLDER
				OES_KASSE	Test af OES_KASSERER
Stat Demo Manual 2	TableData	6	Customer Price Group	OES_BASIS	Test af OES_BASIS
				OES_BOGH	Test af OES_BOGHOLDER
				OES_KASSE	Test af OES_KASSERER
Stat Demo Manual 2	TableData	7	Standard Text	OES_BASIS	Test af OES_BASIS
				OES_BOGH	Test af OES_BOGHOLDER
				OES_KASSE	Test af OES_KASSERER
Stat Demo Manual 2	TableData	8	Language	OES_BASIS	Test af OES_BASIS
				OES_BOGH	Test af OES_BOGHOLDER
				OES_KASSE	Test af OES_KASSERER

Objekter pr. bruger

Rapporten viser en liste over hvilke objekter, brugerne har adgang til.

Objekter pr. bruger

Stat Demo Manual 2

21. august 2003

Side 1

attain

Logon: OES_BOGHOLDER

Bruger-ID	Navn	Objekttype	Objekt-ID	Objekt-navn	Læse	Indsætte	Rette	Slette	Køre
OES_BOGH	Test af OES_BOGHOLDER								
NS_BANK	Redigering af banktabeller	Table Data	232	Finanskladdenavn	Ja	Ja	Ja		
		Table Data	270	Bankkonto	Ja	Ja	Ja		
		Table Data	271	Bankpost	Indirekte	Ja	Indirekt		
		Table Data	272	Checkpost	Indirekte	Ja	Indirekt		
		Table Data	273	Bankkontoafstemning	Ja	Ja	Ja		
		Table Data	274	Bankkto.afstemningslinje	Ja	Ja	Ja		
		Table Data	275	Bankkontoudtog	Ja	Ja	Ja		
		Table Data	276	Bankkontoudtogslinje	Ja	Ja	Ja		
		Table Data	277	Bankbogføringsgruppe	Ja	Ja	Ja		
		NS_BASIS	Læseadgang (basis)	Table Data	3	Betalingsbetingelser	Ja		
Table Data	4			Valuta	Ja				
Table Data	5			Rentebetingelser	Ja				
Table Data	6			Debitorprisgruppe	Ja				
Table Data	7			Tekst	Ja				
Table Data	8			Sprog	Ja				
Table Data	9			Land	Ja				
Table Data	10			Leveringsform	Ja				
Table Data	13			Sælger/Indkøber	Ja				
Table Data	14			Lokation	Ja				
Table Data	15	Finanskonto	Ja						

Best Practise

Som brugeradministrator har man et stort ansvar for sikkerheden i NavisionStat, og det er derfor vigtigt at man løbende kontrollerer rettigheds,- profil,- og brugeropsætningen for uoverensstemmelser og fejl. Dette afsnit gennemgår Økonomistyrelsens anbefalinger, eller best practices, indenfor brugeradministration i Navision Stat. Derudover gennemgås hvilke opsætningsfejl i brugeradministrationsmodulet, der er de mest kritiske, samt hvilke metoder hvormed man kan identificere og udbedre disse fejl. Det skal dog understreges at følgende metoder, ikke nødvendigvis dækker hele institutionens behov for kontrol af sikkerheden i Navision Stat installationen.

Anbefalinger

Følgende anbefaling skal være med til at mindske ressourceforbruget i forbindelse med brugeradministrationen i NavisionStat, og samtidig lette arbejdet med dokumentation i forbindelse med en revision af systemsikkerheden. Endvidere vil eventuelle henvendelser til Økonomistyrelsens support vedrørende rettighedsproblemer desuden kunne løses betydeligt hurtigere, hvis anbefalingerne følges.

”Én profil(eller få) pr. bruger og eventuelt en til flere tillægsroller”.

Der bør så vidt muligt kun tildeles en profil til en bruger. Skal brugeren have yderligere rettigheder der ligger udenfor profilen, bør disse tildeles brugeren som roller. Begrundelsen er bedre overblik over brugernes rollesammensætning, hvilket letter revision af brugeradgangen. Hvis en bruger fx tildeles 4 profiler, kan det være svært at gennemskue, hvilke roller der egentlig er indeholdt, uden at køre rapporter. En undtagelse er standard profilen OES_OPSAET_ALMEN, der netop er oprettet for at samle alle opsætningsrollerne. Denne profil kan med fordel tildeles en bruger, der i forvejen har en anden profil.

”Lokalt oprettede profiler eller roller bør ikke have et navn begyndende med henholdsvis OES_ eller NS_”

Det anbefales at man ikke benytter samme præfiks til lokale profiler og roller som Økonomistyrelsen. Begrundelsen er, at det letter arbejdet med brugeradministration, hvis der ikke skabes tvivl om hvilke profiler og roller der er lokale, og hvilke der er standard. Der opstår desuden ikke risiko navnesammenfald, ved indlæsning af nye rettighedsfiler, der kan ødelægge den lokale opsætning.

”Der bør ikke tildeles nye roller til en standard (OES_)profil”

De standardprofiler der løbende udgives af Økonomistyrelsen bør ikke tilpasses institutionens lokale arbejdsfunktioner. Det vil sige, hvis fx en bogholder i institution ABC, udover standard rollerne i OES_BOGHOLDER, også har behov for NS_BACKUP, skal denne rolle ikke tildeles profilen OES_BOGHOLDER. I stedet skal rollen tildeles hver bogholder, ved siden af profilen, eller der skal oprettes en ny lokal profil fx ABC_BOGHOLDER hvor rollen NS_BACKUP indgår.

Der er flere grunde til denne anbefaling, for det første bliver det hurtigt uigennemskueligt hvilke roller der egentlig er tildelt en bruger, hvis der er manipuleret med standard profilerne. Dette kan give betydeligt ekstra arbejde ved dokumentation, verificering og fejlsøgning af sikkerheden. Derudover umuliggør det ”rensning” af institutionens standard profiler, ved at slette de eksisterende og indlæse nye.

”Der bør ikke ændres i rettighederne i standard (NS_)rollerne ”

Samme retningslinjer gælder for standard rollerne som for profilerne, der bør ikke ændres, tilføjes eller slettes rettigheder i de standard roller der udsendes af Økonomistyrelsen. Hvis der i institutionen er behov for at ændre en rolle bør rettighederne kopieres fra standard rollen, til en ny lokal rolle, og ændres her. Efterfølgende kan den originale standard rolle så udskiftes med den nye lokale kopi. Begrundelsen er den samme, som for ændring i standard profilerne, hvis der manipuleres med standard rollerne, besværliggøres arbejde ved dokumentation, verificering og fejlsøgning af sikkerheden betydeligt.

”Log alle ændringer i rettighedstabellerne”

I Navision Stat finansmodul findes en ændringslog, der kan logge alle indsættelser, ændringer og sletninger i tabellerne. Denne er log er ikke sat aktiv som default, men det anbefales at den aktiveres som minimum på følgende tabeller:

- 2000000005 Rettighed – hvilke rettigheder har hver enkelt rolle
- 2000000002 Bruger – hvilke databasebrugere er oprettet
- 2000000054 Windows-logon – hvilke windows brugere er oprettet
- 6007353 Database-medlem af roller - hvilke roller og profiler er tildelt databasebrugere
- 6007354 Windows-medlem af roller – hvilke roller og profiler er tildelt windowsbrugere

Herefter vil alle ændringer i brugeradministrationsmodulet være dokumenteret i loggen. På denne måde vil dataejereren altid hurtigt kunne afklare eventuelle tvivlsspørgsmål, omkring behandling af data.

Kontrol af tildelte rettigheder

Som nævnt er en vigtig opgave for institutionen, at kunne verificere og dokumentere at brugeradgangen og rettighedshåndteringen er i overensstemmelse med sikkerhedsinstruksen, og gældende sikkerhedskrav. Nedenstående er en hjælp til de sikkerhedsansvarlige, for, på en struktureret måde, at gennemgå rettighedsopsætningen i Navision Stat for uoverensstemmelser.

Hvad skal man være opmærksom på

Herunder gennemgås de mest kritiske fejl, der kan forekomme i Navision. Overordnet er det rettighedsfejl på den enkelte bruger der er interessant, men fejlen kan være opstået på 3 forskellige niveauer:

Rolle - laveste niveau, en rolle har fået tildelt forkerte rettigheder. En fejl her vil gå igen på alle brugere der har fået tildelt rollen. Løsningen er, at rettighederne ændres på rollen, og rettelsen vil automatisk slå igennem på alle brugere med den aktuelle rolle, eller en profil hvor rollen indgår.

Profil - mellemste niveau, en profil har fået tildelt en forkert rolle, og alle brugere der er tildelt denne profil har fejlen. Løsningen er, at rollen fjernes fra profilen, og rettelsen vil automatisk slå igennem på alle brugere med den aktuelle profil.

Bruger - højeste niveau, brugeren har fået en forkert sammensætning af profiler og roller. Løsningen er, at sammensætningen ændres, og rettelsen gælder kun for den aktuelle bruger.

Fremgangsmåde :

- 1) Identificer de roller har kritiske rettigheder :
 - a. Kørsels rettigheder til Codeunit 6006951(klarmelding) og samtidig 6006952(bogføring) (ingen roller må have denne kombination)
 - b. Læse, skrive, redigere eller sletterettigheder i TableData = 0 (kun SUPER og SUPER(DATA))
 - c. Kørselsrettigheder til Codeunit = 0 (kun SUPER, NS_REVISION og NS_TEKNIK)
 - d. Skrive, slette, redigererettigheder til TableData = 6016812, 6016813 eller 6016814(kun NS_OPS_PROKURA)
 - e. Læserettigheder til personaledata TableData = 6007063 (kun NS_SLS_SE og NS_MEDARB_SE)
 - f. Læserettigheder til løndata TableData = 5200 (kun NS_SLS_SE og NS_MEDARB_SE og NS_TIDSREG)

Hvis der identificeres standard roller, udover de angivne, der har en eller flere af de kritiske rettigheder, skal de slettes. Hvis der identificeres lokale roller der har en eller flere af de kritiske rettigheder, skal det fremgå tydeligt af sikkerhedsinstruksen, hvorfor disse er oprettet.

- 2) Identificer usikre og 'ulovlige' profiler. Usikre profiler indeholder roller med kritiske rettigheder. For standardrollerne drejer det sig om nedenstående.:

NS_BOGHOLDER
NS_KASSERER
NS_PROKURA
NS_TEKNIK
NS_REVISION
NS_MEDARB_RED
NS_MEDARB_SE
NS_SLS_SE
SUPER
SUPER(DATA)

De lokale roller med kritiske rettigheder er blevet identificeret under pkt. 1).

'Ulovlige' profiler indeholder roller der ikke må kombineres. Det vil sige en profil der er sammensat af roller, der tilsammen muliggør både klarmelding og bogføring eller adgang til alle objekter. For standardrollerne drejer det sig om nedenstående rollesammensætninger, der ikke må forefindes i samme profil. Derudover skal institutionens lokale usikre roller også medregnes:

NS_BOGHOLDER og NS_KASSERER
(NS_BOGHOLDER eller NS_KASSERER) og (NS_TEKNIK eller
NS_REVISION)
(SUPER eller SUPER(DATA)) og alle øvrige roller

Herudover bør rollen NS_OPS_PROKURA ikke indgå i nogen profil.

Hvis der identificeres 'ulovlige' profiler, skal den, eller de usikre roller fjernes, således at der ikke længere er konflikt i kombinationen af roller.

- 3) Identificer de brugere der har en 'ulovlig' sammensætning af de identificerede usikre profiler eller usikre roller, ex en bruger der har profilen OES_BOGHOLDER og samtidig rollen NS_REVISION. Her skal man dog være opmærksom om en rolle eller profil er betinget til ét specifikt regnskab, hvorved der ikke opstår rettighedskonflikt.
- 4) Hvis én bruger har flere login til Navision bør det kontrolleres, at disse login ikke indgår i to forskellige prokuragrupper til samme bank og bankcentral. Hvis dette er tilfældet kan en fysisk bruger både 1. og 2. godkende betalinger til NemKonto.

Det kan kontrolleres via stien: Finans/Bank/Bankkonto/Brugere. Her kan man se om en bruger med flere login er sat op i to forskellige grupper til samme bankcentral. Ex: administratoren ved at en bruger har to login til Navision(PBB og PLB), i figuren ses at disse login har hver deres Prokuaregruppekode til samme Bankcentral kode, dette bør ikke forekomme.

Bruger-ID	Bankcentral kode	Prokuragruppekode
AKL	NKS	GRUPPE1
IGT	JB01	GRUPPE1
PBB	NKS	GRUPPE1
PLB	NKS	GRUPPE2

Hvordan identificerer man de kritiske fejl

Herunder gennemgås hvilke muligheder der er i Navision Stat, for at kunne verificere og dokumentere at de tidligere nævnte kritiske fejl ikke optræder i systemet. Der tages udgangspunkt i de tre niveauer, rolle, profil og bruger.

På rolleniveau:

Kør rapporten 'Rettigheder pr. rettighedsgrp' hvor der indsættes ekstra anfordringsoptioner 'Objekt-ID' og 'Objekttype'. Dette gøres ved at markere rapporten og tryk 'Udskriv'. I anfordringsvinduet(filtervinduet), stå i en tom række i kolonen 'Felt', og tryk på 'drill-down' pilen og vælg de ekstra felter ind. Herefter kan man få en rapport over hvilke roller der har hvilke rettigheder. Denne rapport er god til at begrænse resultaterne, selvom der udskrives for alle roller.

På profilniveau:

Via stien Brugeradministration/Opsætning/menuknap 'Profil'/menupunkt 'Pr.profil', fås en samlet oversigt over hvilke roller der indgår i hver enkelt profil. Denne metode giver et godt overblik, men kan være for uoverskuelig. Evt. resultater skal udlæses til eksternt program ex. Excel, og gennemgås manuelt. Eller kør rapporten 'Roller pr. profil' der viser for hver profil, hvilke roller der er tilknyttet. Resultatet skal efterfølgende gennemgås manuelt.

På brugerniveau:

Via stien Brugeradministration/Database-login(eller Windows-login) /menuknappen 'Rettigheder' ses brugerens profiler og roller. Denne metode er mest brugbar, hvis det er én konkret bruger man ønsker at kontrollere. Eller kør rapporten 'Roller pr. bruger' hvor der indsættes ekstra anfordringsoptioner 'Rolle-ID'. Dette gøres ved at markere rapporten og trykke 'Udskriv'. I anfordringsvinduet(filtervinduet) indsættes ønskede nye felter. Tryk på 'drill-down' pilen og vælg ønskede felter ind. Dette skal gøres på både database- og windowsbrugerfanebladet. Herved kan man filtrere på de usikre roller, man ønsker at kontrollere fx NS_KASSERER og NS_BOGHOLDER. Rapporten giver et godt overblik over brugerne med kritiske roller, men viser ikke profiler.