

UNIQUE SECURITY

ANSATT MED GRUPPER

INNHALDSFORTEGNELSE

1. HVORFOR BRUKE UNIQUE SECURITY?	3
2. BEGREPER I SECURITY	4
2.1. SYSTEM / LØSNING.....	4
2.2. APPLIKASJON.....	4
2.3. RESSURSER:	4
2.4. BRUKERE	4
2.5. SECURITY ADMINISTRATOR.....	5
2.6. SYSTEM ADMINISTRATOR.....	5
2.7. SYSTEM REVISOR	5
2.8. TILGANG	5
3. UNIQUE SECURITY MOT UNIQUE ANSATT	6
3.1. FORUTSETNINGER.....	7
3.2. SYSTEM	8
3.3. STATUS	8
3.4. STANDARDTILGANG.....	8
3.5. RESSURSER	8
3.6. BRUKERGRUPPER.....	8
3.7. OVERSIKT TILGANG	<i>FEIL! BOKMERKE ER IKKE DEFINERT.</i>
4. OPPRETTE GRUPPER	9
5. LEGGE BRUKERE INN I GRUPPER	10
6. LEGGE INN APPLIKASJONER (PROGRAMMER)	11
7. LEGGE INN BRUKERDEFINERTE RESSURSER	14
7.1. TILGANG TIL Å KJØRE ELLER LAGE RAPPORTER	14
7.2. TILGANG TIL FANENE I BILDET STILLING M/FASTLØNN	17
7.3. MULIGHET FOR Å ”LÅSE” EN AV ROLLENE I ÅPNINGSBILDET.....	18
8. TILGANG	20
8.1. HVOR KAN TILGANG TILDELES.....	20
8.2. PRIORITET	20
8.3. TILGANG FLERE GRUPPER.....	20
9. GLEMT PASSORD ?	21
9.1. BRUKER.....	21
9.2. SYSTEM ADMINISTRATOR.....	21
9.3. SECURITY ADMINISTRATOR.....	21
10. FORSLAG TIL ”HOVEDGRUPPER OG FAGGRUPPER”	22

1. HVORFOR BRUKE UNIQUE SECURITY?

Konsesjonsvilkårene for å kjøre system, særlov, forvaltnings- og offentlighet lov stiller alle krav til sikkerheten ved systemet.

Hensikten med **Unique SECURITY** er å regulere tilgangen brukere har til ressurser i Unique systemer. Unique SECURITY kommer i tillegg til de sikkerhetstiltak en kan foreta fysisk (låsing av lokaler, rom, skriver), via operativsystem (tilgang til maskin, time - out, tilgang til kataloger og filer), og tilgang som regulerer med spesielle applikasjoner tilhørende systemet som tildeler og begrenser adgang etc.. For alle Unique systemer gjelder at de kan settes opp slik at en hindrer muligheten å starte opp applikasjoner utenfor systemet (closed - system = ON).

Unique Security er delt inn i to områder, Security administrator og System administrator. Stort sett tar Security adm. seg av brukerdefinisjoner og systemtilgang, mens System adm. tar seg av tilgang for brukergrupper og applikasjoner.

Som nevnt nedenfor er Security administrator som regel dekket med en person fra drifts/it -avdelingen. Det anbefales egne kurs for disse fra en teknisk konsulent fra Webcenter Unique.

I denne sammenheng må vi også nevne et menyvalg som ligger i Unique Ansatt. Under **Standard / Brukervariable / Bruker adgangskontroll** er det også mulig å regulere tilgang for de enkelte brukere. Her styres tilgang for eksempel etter avdeling (ansvar), etter ansattnr., utbetalingssted etc. Her angis fra- og til for det man skal ha tilgang til, slik at man kun får tilgang til "egne" data, data for ansatte man har arbeidsoppgaver imot.

Dette kurset vil ta for seg oppgavene en System administrator må beherske.

2. BEGREPER I SECURITY

2.1. SYSTEM / LØSNING

- Et system er et sett av Unique program. For eksempel ANSATT, ØKONOMI, KOMMFAKT.

2.2. APPLIKASJON

- Et program, et skjermbilde eller rapport.

2.3. RESSURSER:

- Systemoppgaver. Eks. DEBUGGER (verktøy for å undersøke system og applikasjoner), QUICK (verktøy for å lage nye applikasjoner) og XTRA (verktøy for å lage rapporter) Applikasjoner (skjermbilder og rapporter m.m.)
- Applikasjoner (skjermbilder og rapporter m.m.
Brukerdefinerte ressurser. Med dette menes at du kan definere egne brukerattributter. Finnes i Unique ANSATT.

BRUKER DEFINERTE RESSURSER

Egentlig er dette en variabel som for hver brukergruppe kan gis en viss verdi i Security. Ut fra denne verdien kan programmet finne ut hva den enkelte brukeren har lov til å gjøre. For eksempel har vi den brukerdefinerte ressursen FORHANDLING, som kan settes til ADMIN eller BRUKER. De som har fått verdien ADMIN, har alle rettigheter i modulen for Lokale forhandlinger. Det har ikke de som får verdien BRUKER, de får bl.a. ikke se menypanelet Grunndata.

2.4. BRUKERGRUPPER

Vi opererer med BRUKERGRUPPER nå vi tildeler tilgang til systemet. Det letter vedlikeholdet når vi får inn nyansatte eller man skifter på arbeidsoppgavene. Det er adskillig lettere å melde brukere ut av / inn i disse gruppene, enn å måtte definere komplett tilgang for hver bruker.

2.5. BRUKERE

- Med brukere menes de som er registrert som brukere av systemet. Brukere av systemene må defineres i Security-administrator, og bør defineres med Brukernavn lik Login id på Unix/NT server (slippes da inn i Ansatt uten ny pålogging).
- Brukere må i tillegg registreres under **Standard / Brukervariable / Brukerinformasjon** (siden dette er en del av Unique Ansatt og ikke av Security). Brukerid. her (max. 8 tegn) må enten være lik Brukernavn fra Security, evt lik det som er registrert under initialer samme sted.

2.6. SECURITY ADMINISTRATOR

- Opprette systemer, f.eks. Unique ØKONOMI, Unique ANSATT etc.
- Registrere alle brukere som skal ha tilgang til systemene.
- I tillegg bestemmer Security administrator hvem andre brukere som skal være Security / System administrator eller System revisor.
- Anbefales person fra drifts – avdeling
- Tildeler passord til brukere
- Gir tilgang til selskap

Dette er oppgaver som oftest blir ivaretatt av it-avdelingen.

2.7. SYSTEM ADMINISTRATOR

- Lager brukergrupper og knytter brukerne til aktuelle grupper.
- Legger inn applikasjoner.
- Definerer tilgang til grupper, brukere eller applikasjoner
- Administrerer logger
- Definerer hvem andre som skal være System administrator eller System revisor på sitt system.

Dette er oppgaver som vanligvis blir ivaretatt av systemansvarlig for Uq Ansatt, samtidig som man har en reserve eller to i tilfelle fravær og ferier.

2.8. SYSTEM REVISOR

- Sjekker at tilgang er gitt til de som trenger det, samt at vesentlige og sensitive data er skjermet fra unødvendig innsyn utenfra
- Sjekker logger

Det er mulig å være Security- og System administrator samtidig. Det er også mulig å være Systemadministrator for flere systemer. Det er derimot ikke mulig å være både Systemadministrator og Systemrevisor på samme system.

2.9. TILGANG

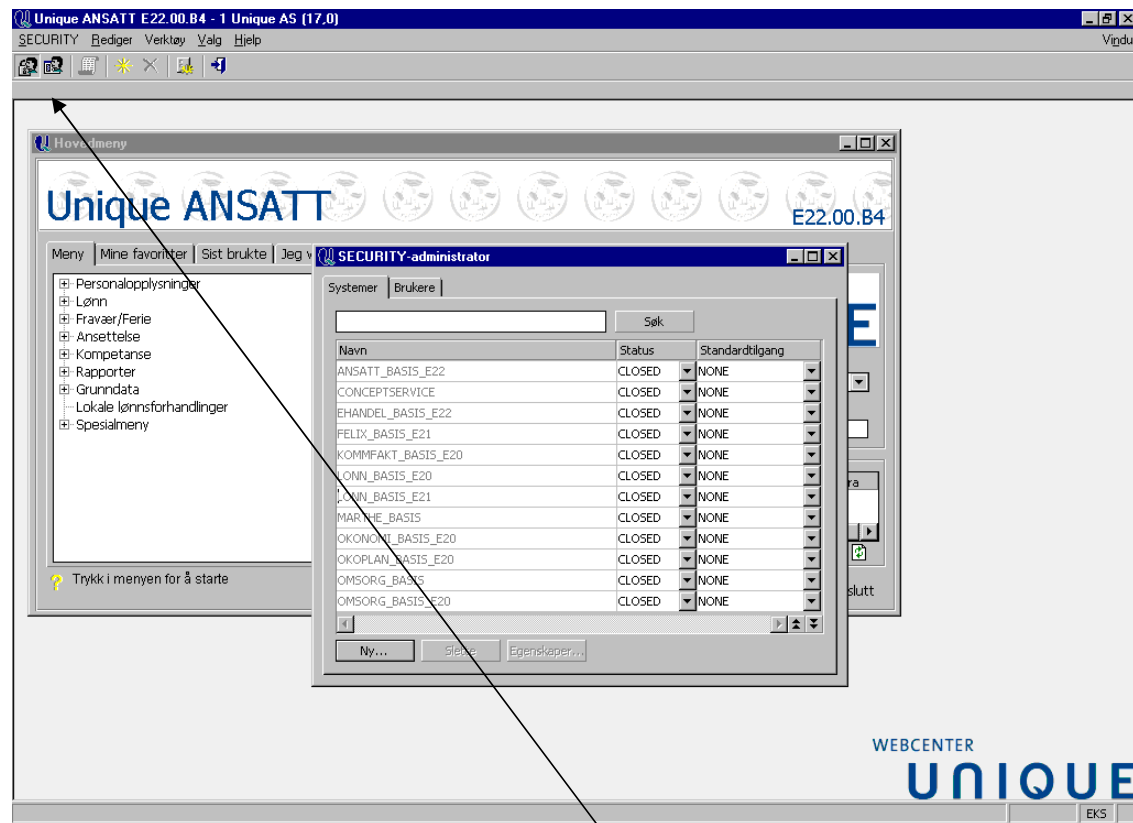
For brukergrupper, applikasjoner og systemer er tilgangen gradert slik:

- Ingen tilgang (NONE)
- Spørre/lesetilgang (QUERY)
- Oppdatering (UPDATE)
- Innsetting (INSERT)
- Slette data (DELETE)

Det er vanligvis tilstrekkelig om man benytter (NONE), (QUERY) og (DELETE).

3. UNIQUE SECURITY MOT UNIQUE ANSATT

Menyvalg : Diverse - Security



Øverst i bildet finnes en knapp rad. De 2 knappene til venstre betegner om du er innlogget / definert i Unique Security som Security administrator eller System administrator.

Knappen til venstre er Security administrator og den neste er System administrator. Her vil kun en knapp være tilgjengelig hvis brukeren ikke har tilgang til begge rollene.

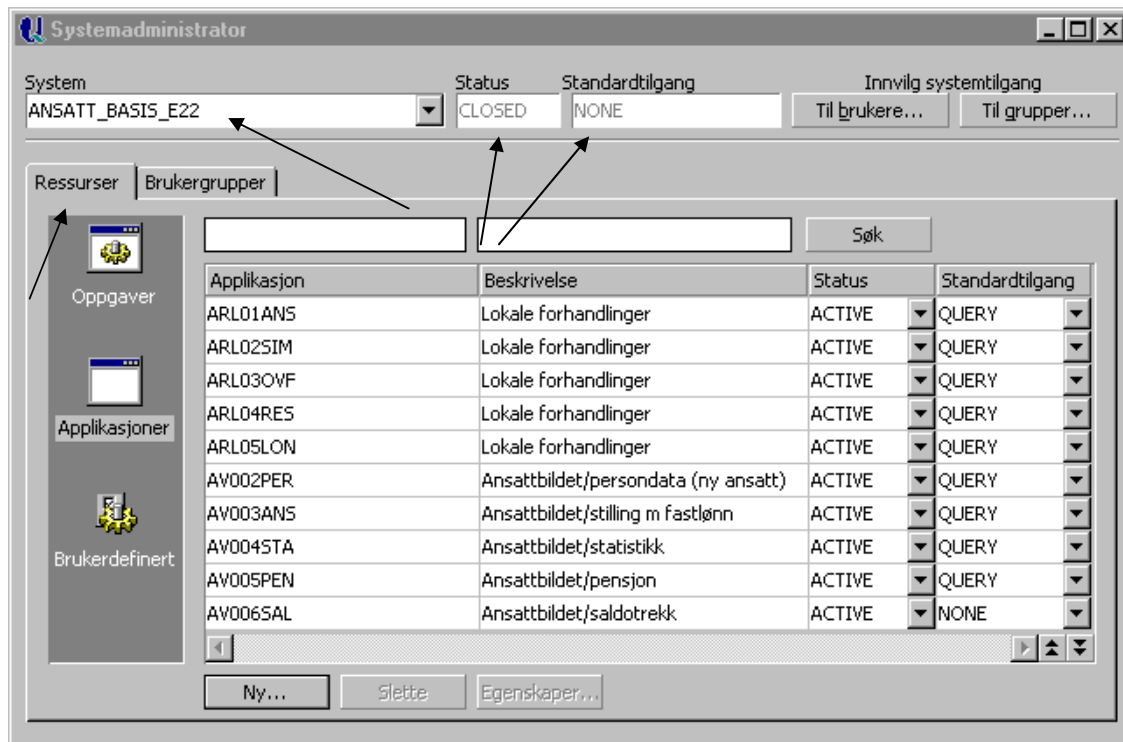
Når et system blir opprettet i Unique Security, skal det tildeles en standardtilgang og en status. Standardtilgangen kan være None og status kan stå til
OPEN krever ikke at brukeren er definert med egen tilgang
CLOSED sjekker om brukeren er definert opp mot aktuelt system

Hvis status da står til OPEN vil Security lete etter brukeren om den er opprettet generelt i Security, hvis ja, slippes brukeren inn og får tilgang på evt. gruppen den er medlem av. Hvis han ikke er medlem av en gruppe får brukeren tilgangen som systemet har. Hvis den er satt til None blir brukeren følgelig kastet ut av løsningen. Hvis systemet er satt til CLOSED vil brukeren kun slippe inn hvis den er medlem i en gruppe i systemet.

3.1. FORUTSETNINGER

Vi forutsetter nå at Security administrator har opprettet Unique ANSATT som system, og at brukerne er registrert inn med samme brukernavn som de har på Unix/NT server.

Nå er vi logget på som System administrator:



Feltene som pilene peker på , er forklart på neste side.

NB! ... QUERY eller (QUERY).

Tilgang kan være oppgitt med eller uten parentes.

Førstnevnte betyr at tilgang er satt spesifikt for denne enheten, som for applikasjon ovenfor, mens tilgang i parentes ikke er satt, men "arvet" fra nivået ovenfor (for eksempel når en bruker får tilgangen til den gruppen vedkommende er medlem i).

3.2. SYSTEM

- viser hvilket system som du nå jobber mot

3.3. STATUS

- viser den status systemet har fått tildelt av Security administrator
 - **OPEN** krever ikke at brukeren er definert med tilgang
 - **CLOSED** sjekker bruker og krever definert tilgang
 - **PASSIVE** for vedlikehold , for eksempel database
 - **SUPERVISOR** det er kun mulig for supervisor å komme inn

3.4. STANDARDTILGANG

- viser standard tilgang, satt på systemet av Security administrator

Et system i drift bør ha status CLOSED og standard tilgang NONE

3.5. RESSURSER

- oppgaver Verktøy som Debugger, Quick og Xtra
- applikasjoner Skjermbilder og tabeller
- brukerdefinert Brukerdefinerte attributter, rapportgeneratoren.

3.6. BRUKERGRUPPER

For at en brukergruppe skal fungere som vi forutsetter, er det fem arbeidsoppgaver vi må gjennomgå :

1. Opprett en ny Brukergruppe
2. Innvilg generell systemtilgang for gruppen
3. Kryss av for de brukerne som skal være medlem av gruppen
4. Finn ut hvilke applikasjoner eller programmer disse brukerne trenger utvidet eller redusert tilgang til (i forhold til gruppens generelle tilgang). Sjekk at disse programmene er registrert under **Ressurser / Applikasjoner**. Hvis ikke registrer dem og gi systemtilgang **SYSTEM**.
5. Sett markøren på applikasjonen du la inn, bruk **høyre musetast** og få oversikt over alle gruppene m/den tilgang de har til nevnte applikasjon. Foreta nødvendige endringer for den gruppen du jobber med.

4. OPPRETTE GRUPPER

Det første vi skal begynne med er å opprette de brukergruppene vi mener vi har behov for. Bakgrunnen for dette er at vi har en gruppe brukere som skal ha samme rettighetene på et system. Ved å opprette grupper får man en enklere administrasjon, bedre oversikt og det øker sikkerheten. Det anbefales at det er laget en matrise på forhånd. Denne bør inneholde følgende:

- Grupper og standard tilgang til disse
- Medlemmer til de ulike gruppene
- Applikasjoner knyttet til de ulike gruppene

- 1) Velg mappen 'Brukergrupper' og klikk på knappen 'Ny'.
- 2) Legg inn navnet på gruppen. Status skal stå til Active.
- 3) Tildel standardtilgang for Brukergruppen ved hjelp av knappen (Innvilg tilgang) **'Til grupper'** øverst til høyre i bildet.

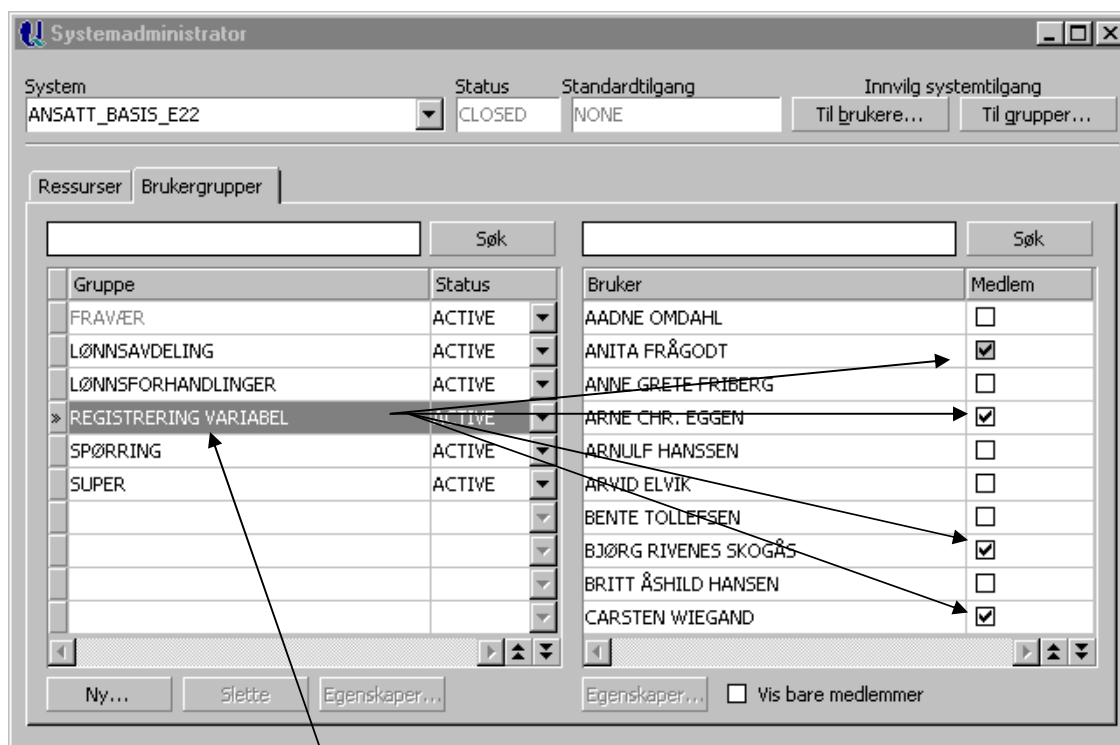


- Opprett de andre gruppene på samme måte. Ved å klikke på knappen 'Til grupper', kan tildelte standard tilgang endres.
- Nå er gruppene klare for å melde inn brukere. Vi anbefaler IKKE å gi tilgang direkte til en bruker.

NB! Husk alltid å gi gruppen en tilgang. Hvis det ikke settes tilgang vil gruppen "arve" den tilgangen som systemet er satt opp med. I de fleste tilfeller vil da systemtilgangen være (None).

5. LEGGE BRUKERE INN I GRUPPER.

Brukerne er allerede opprettet av Security administrator. Nå skal disse brukerne knyttes til grupper for å få korrekt tilgang til systemet. Vi anbefaler ikke å legge tilgang direkte på en bruker. Dette for å enkelt kunne legge nye brukere inn i systemet uten å måtte definere de samme tilganger som tidligere er gitt. Gjelder spesielt hvis en person skal erstatte en gammel bruker. Det er da enklere å slette den gamle brukeren og legge inn den nye i en gruppe, fremfor å slette den gamle og deretter definere opp de samme tilgangene på den nye brukeren.

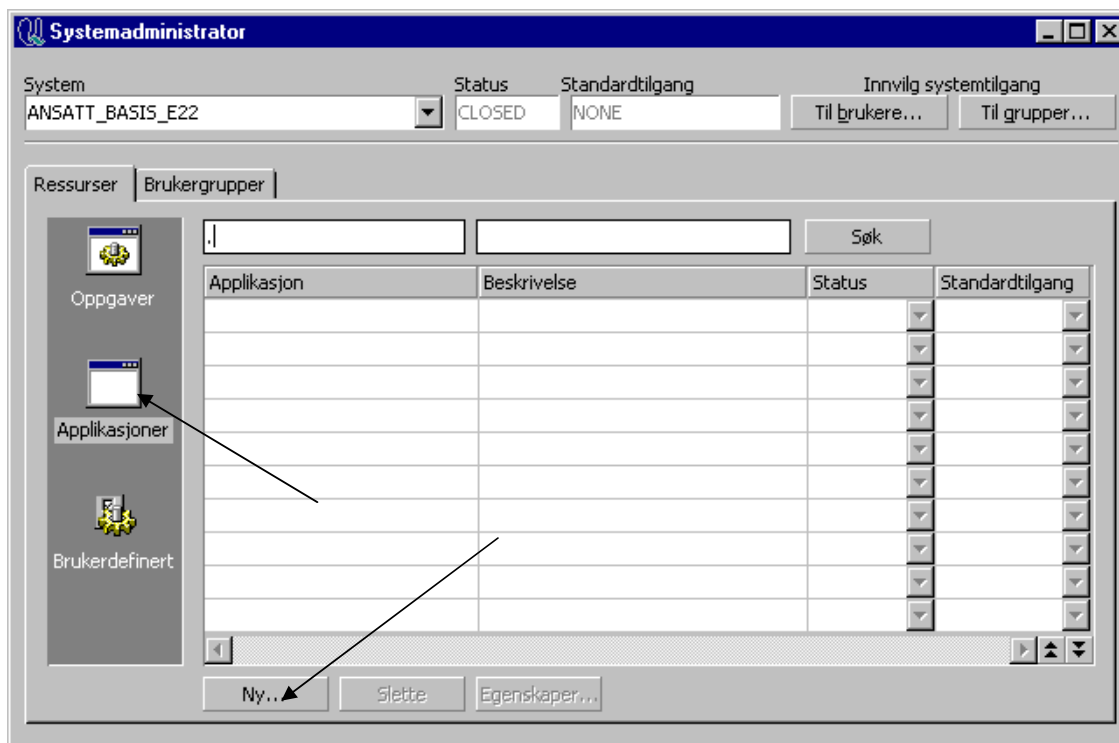


- Klikk på ønsket gruppe og den blir merket til venstre for teksten (se pil)
- Huk deretter av for de brukerne som skal være medlem i de respektive gruppene. (se pil til høyre i bildet)
- Når man ønsker å se hvem som er medlemmer hvor, kan man velge å kun se tilhørende medlemmer til en gruppe (Kryss av for "Vis bare medlemmer").
- En bruker kan være medlem i en eller flere Brukergrupper. Hvis det er behov for at en bruker skal være medlem i flere grupper må Security settes opp med en annen konfigurasjon. ("Handle Multiple Membership" i Security administrator).

6. LEGGE INN APPLIKASJONER (PROGRAMMER)

For å kunne styre tilgangen ytterligere enn på brukergruppe nivå, må vi legge inn de menyvalgene vi ønsker en annen tilgang på. Et system inneholder mange applikasjoner. Vi kan velge mellom å legge inn alle, ingen eller enkelte. Hva man velger avhenger av faktorer som vedlikehold, oversikt, antall brukere osv. Det kan gjøres manuelt eller leses inn via en laste jobb. Generelt forenkler det vel vedlikeholdet når man kun legger inn de applikasjonene som er nødvendig. Mao. applikasjoner som skal ha en annen tilgang enn det som gruppen generelt har.

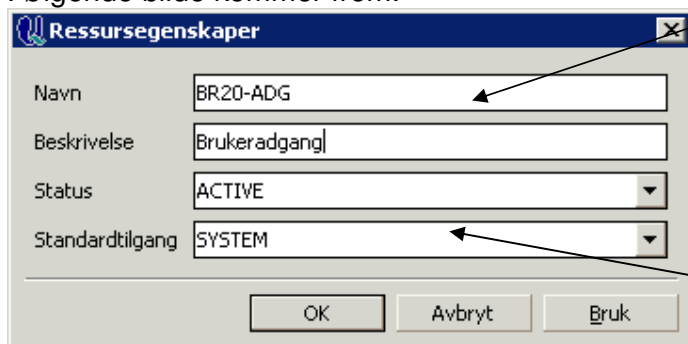
Vi skal nå se på hvordan dette gjøres i registreringsbildet for applikasjoner:



Vi står nå i fanen 'Ressurser', og merker valget 'Applikasjoner'

- Klikk på knappen 'Ny'

Følgende bilde kommer frem.



Eks.
BR20-ADG er navnet
for brukeradgang i
Ansatt.

Gi standardtilgang
til applikasjonen

Legg inn navnet på skjermbildet .

- Gi standard eller generell tilgang på skjermbildet / rapporten

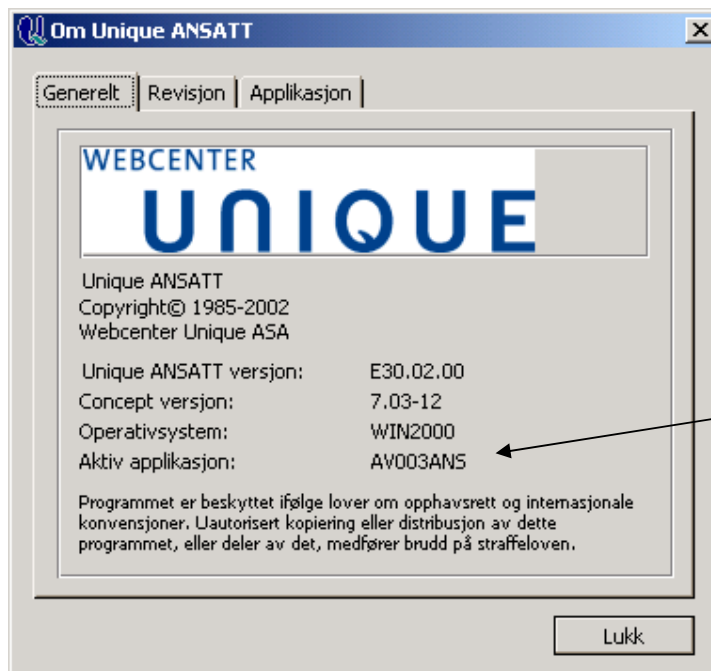
Den tilgang vi har registrert på innmeldt applikasjon, kan senere overstyres på den enkelte brukergruppe. Det kan derfor være lurt å benytte standardtilgang **SYSTEM**. Dette medfører at applikasjonen legges inn på brukergruppene med den samme tilgang som gruppen har. En gruppe med Query-tilgang får da Query-tilgang til BR20-ADG, mens Supergruppen som har Delete, får Delete til dette programmet.

Å justere tilgang til applikasjonen for gruppene.

De applikasjonene vi nå legger inn, må vurderes i forhold til alle brukergruppene. Vi setter markøren på aktuell applikasjon, bruker høyre museknapp og velger menyvalget 'Innvilg tilgang' og deretter 'Til brukergruppe'. Nå kan vi sette opp tilgangen for denne gruppen vi jobber med, evt redusere eller fjerne tilgangen helt. I dette bildet har du også mulighet for å kontrollere de øvrige gruppenes tilgang.

Hvordan finne navn på applikasjonen ...?

- Start applikasjonen fra menyen. Bruk "Hjelp" på øverste menylinje (hovedmeny). Velg videre: "Om Unique Ansatt":

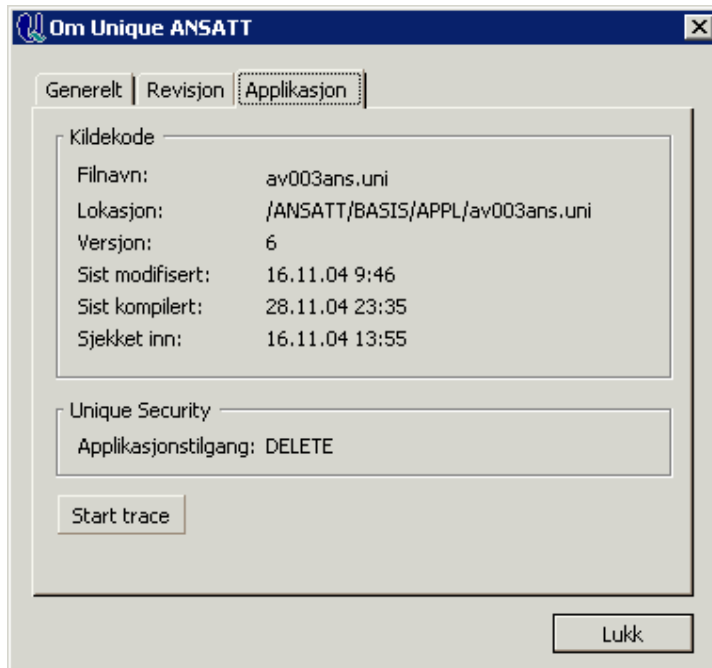


Eks. på programnavn for skjermbildet **Stilling med fastlønn**.

Det er dette applikasjonsnavnet som legges inn i Security. **Navn legges ikke inn med "etternavn" (extension), vi tar bare med av003ans.**

Hvordan sjekke tilgangen til en applikasjonen ...?

I det samme bildet kan du også sjekke hvilken tilgang du har til en applikasjon. Det kan være nyttig hvis det dukker opp problemer med tilgangen. Trykk på fanen **Applikasjon**.

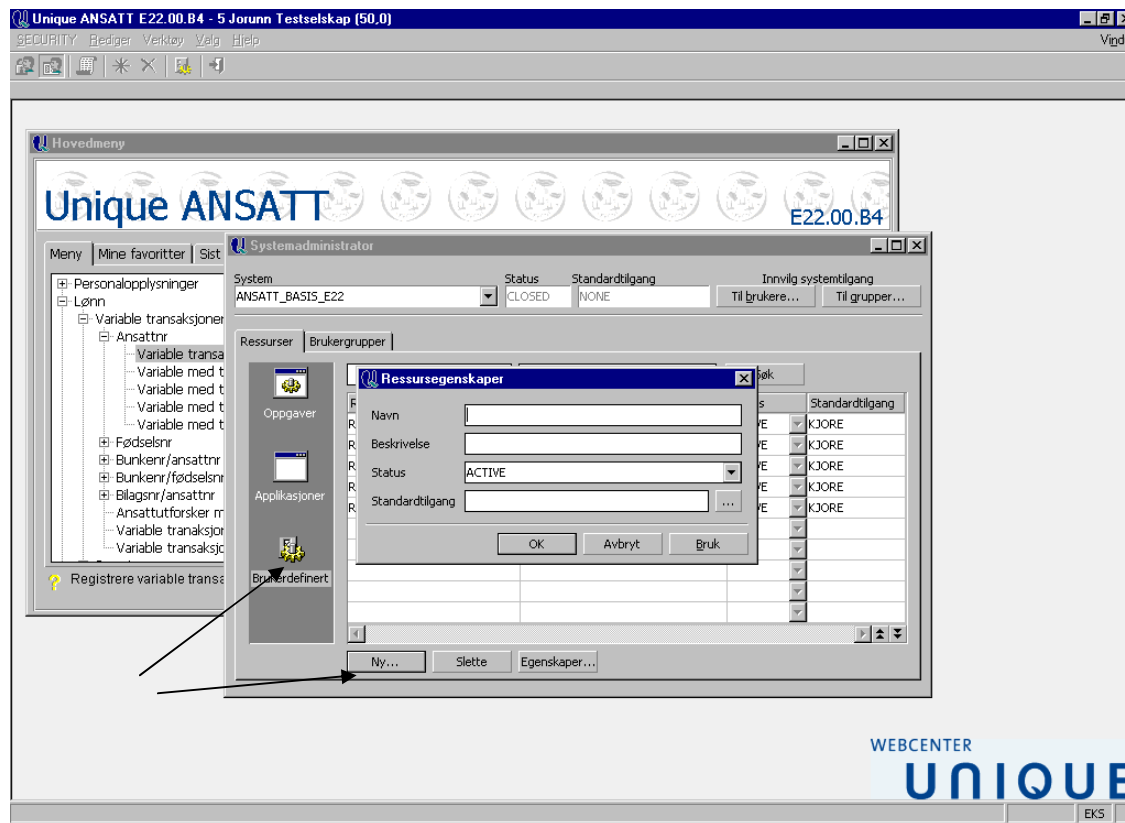


Her finner du en Security-boks hvor din tilgang til nevnte program er oppgitt.

7. LEGGE INN BRUKERDEFINERTE RESSURSER

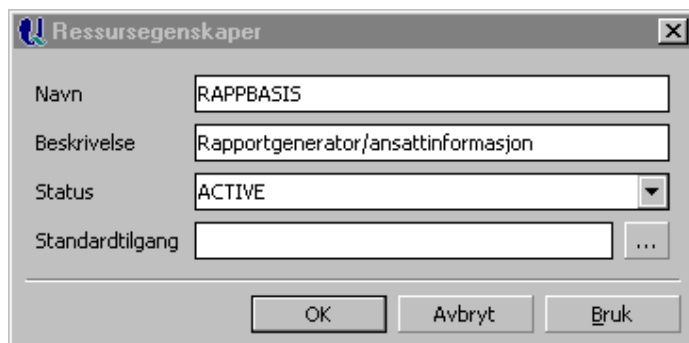
7.1. TILGANG TIL Å KJØRE ELLER LAGE RAPPORTER

OBS. Gjelder ikke for ny Rapportgenerator fra versjon E32 (se kap. 7.2).



Prinsippielt behandles brukerdefinerte ressurser omtrent på samme måte som Applikasjoner. Velg "ny" og bildet for ressursegenskaper fremkommer. Skriv inn navn på ressurs, for eksempel rapporttypen RAPPBASIS (rapporttype som gir tilgang til basisopplysninger fra Persondatatabilene). I dette bildet kan man ikke velge standardtilganger slik man gjør med applikasjoner. Vi må selv definere hvilke tilganger vi ønsker å benytte. Her kan vi velge mellom KJORE og LAGE, og gir hhv. mulighet for og kjøre rapporter og lage egne, nye rapporter, i tillegg til INGEN.

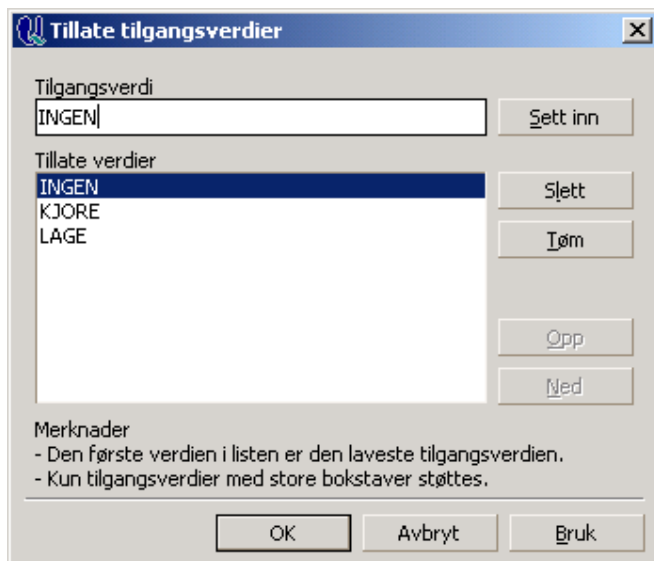
Klikk på knappen bak "Standardtilgang"



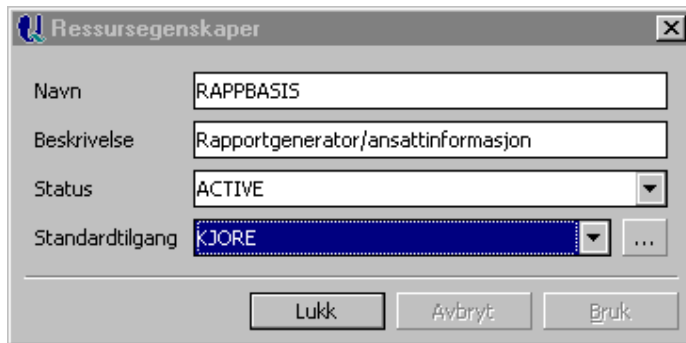
Følgende skjermbilde fremkommer.



Her må tilgangsverdier skrives inn slik at de fremkommer i listen. Start med lavest tilgang. **NB!** Det er **meget viktig** at man legger inn verdi med lavest tilgang først i de tilfeller man benytter muligheten for at brukere skal ligge i flere grupper.



Trykk så "OK" og velg evt. en annen tilgang enn den som fremkommer.

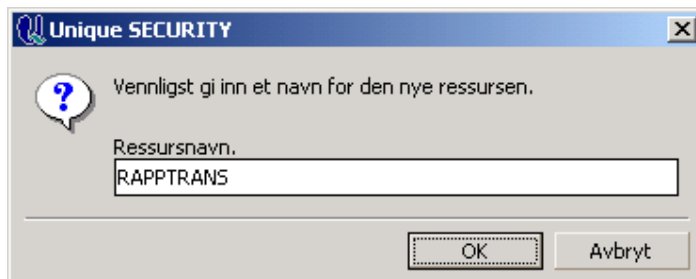


Du har nå definert en ressurs.

For å legge inn flere ressurser gjør man det på samme måte. Det kan oppleves som tungvint at man for hver ny ressurs må skrive inn tilganger KJORE og LAGE. Det finnes en mulighet å kopiere disse.

Kopiering gjøres som følger:

Stå på en ressurs som det er definert inn standardtilganger på. Høyreklikk med muspeker og velg "kopier innførsel" man får da mulighet til å legge inn navn på ny ressurs, hvor tilgang (KJORE, LAGE) følger med i ny kopi.



Husk å angi standardtilgang på ressursene etter at de er opprettet.

Øvrige rapporttyper som må defineres på denne måten:

- RAPPTRANS - rapporter m/tilgang til lønnstransaksjoner
- RAPPFRAV - rapporter m/tilgang til fraværstranser
- RAPPFERIE - rapporter m/tilgang til ferieregistrering
- RAPPKOMP - rapporter m/tilgang til reg. kompetanse

7.2. TILGANG I NY RAPPORTGENERATOR – E32.

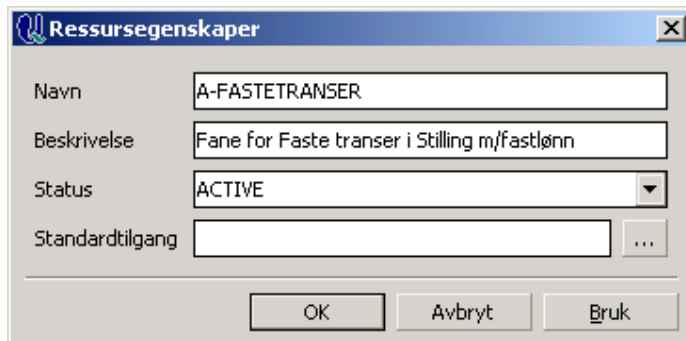
I den nye rapportgeneratoren er dette forenklet en del. Nå styres tilgangen ved å gi tilgang til selve programmet, SR01-HOV, brukerdefinerte ressurser brukes ikke lenger.

Delete-tilgang til SR01-HOV gir mulighet for å lage og kjøre alle typer rapporter. Query-tilgang gir bare mulighet til å kjøre eksisterende rapporter, ikke endre på dem.

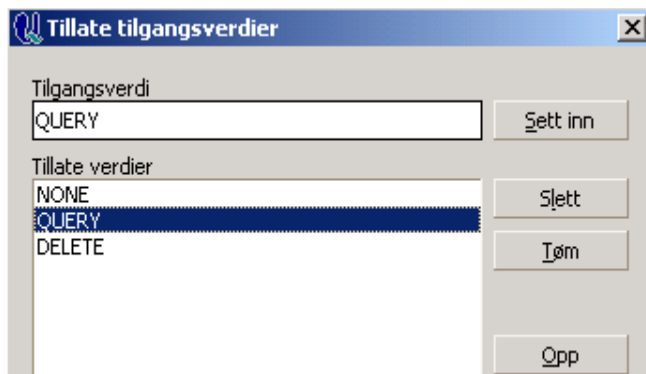
7.3. TILGANG TIL FANENE I BILDET STILLING M/FASTLØNN

Enkelte kunder kan ha behov for å skjerme deler av skjermbildet Stilling m/fastlønn. Det kan for eksempel være å hindre registrering eller endring av faste transer, eller hindre innsyn til fanen Lønnsopplysninger. Dette kan legges inn under Brukerdefinerte ressurser.

De nevnte fanene heter hhv. A-FASTETRANSER og A-LONNSOPPL og tilgang må defineres som for rapportene i forrige avsnitt, men her med de vanlige alternativ for tilgang, None, Query og Delete.



Trykk på knappen bak Standardtilgang for å legge inn de aktuelle alternativene.

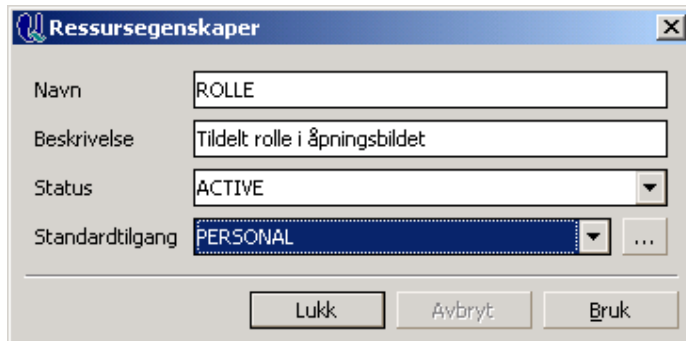


Og gjør tilsvarende for den andre fanen.



7.4. MULIGHET FOR Å "LÅSE" EN AV ROLLENE I ÅPNINGSBILDET

I åpningsbildet er det mulig å velge forskjellige roller for bruk av systemet. Dette påvirker menyen du får tilgang til. Har du satt på rolle Personal er de typiske menypunktene for Lønn tatt ut. Med rolle Lønn forsvinner menypunktene som har med Personal og gjøre. Rolle Ansatt dekker alle menypunkter. Under Brukerdefinerte ressurser kan du nå "låse" en gruppe til en av disse rollene, slik at muligheten for å endre tildelt rolle forsvinner. Da må du legge inn ressursen Rolle.



Ressursegenskaper

Navn: ROLLE

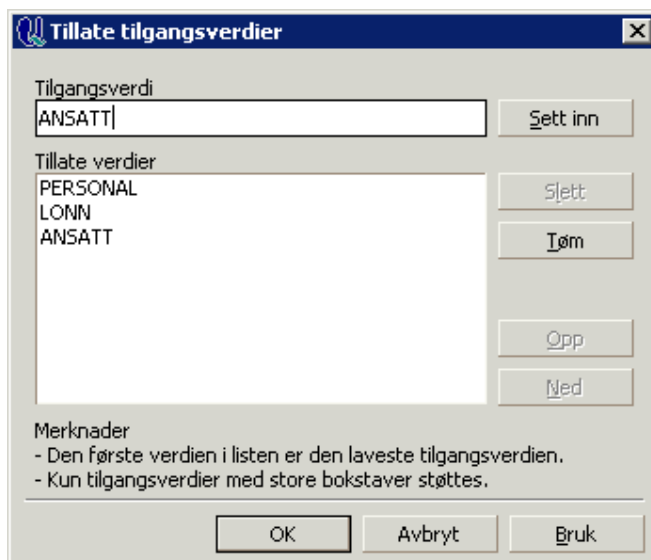
Beskrivelse: Tildelt rolle i åpningsbildet

Status: ACTIVE

Standardtilgang: PERSONAL

Lukk Avbryt Bruk

Som i forrige avsnitt legges alternativene inn under knappen bak Standardtilgang.



Tillate tilgangsverdier

Tilgangsverdi: ANSATT

Tillate verdier: PERSONAL, LONN, ANSATT

Merknader:
- Den første verdien i listen er den laveste tilgangsverdien.
- Kun tilgangsverdier med store bokstaver støttes.

Sett inn Slett Tøm Opp Ned

OK Avbryt Bruk

Nå kan du for den enkelte gruppe gå inn og sette tilgang til Rolle, slik at de kun får tilgang til menypunktene innenfor Lønn eller Personal. **(Merk at Lønn leggs inn som LONN).**

7.5. BRUKERDEFINERT TILGANG I LOKALE FORHANDLINGER.

Vi har også en brukerdefinert ressurs FORHANDLING, som benyttes til å styre tilgangen til Lokale Lønnsforhandlinger.

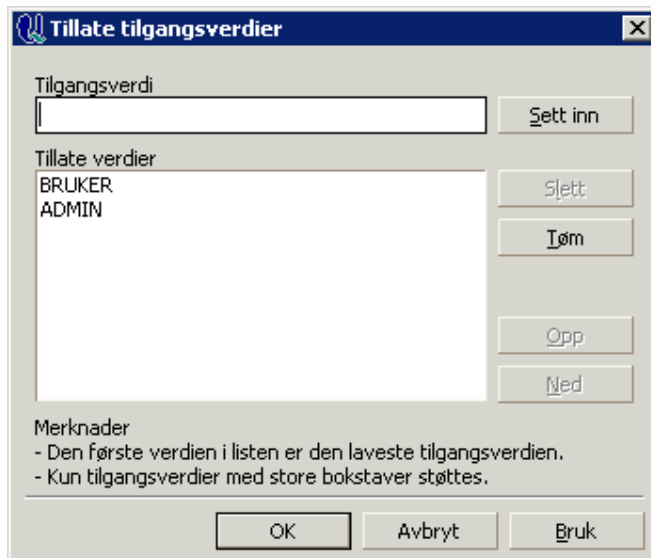
Den skiller mellom den/de som er administrator for forhandlingsmodulen og de som bare skal inn og registrere krav og/eller tilbud. Sistnevnte får for eksempel ikke tilgang til Grunndata. De får heller ikke tilgang til menypunktet for å overføre det endelige forhandlingsresultatet tilbake til Lønn.

Førstnevnte gruppe gis tilgang ADMIN, den andre får BRUKER.



The 'Ressursegenskaper' dialog box contains the following fields and controls:

- Navn: FORHANDLING
- Beskrivelse: Lokale forhandlinger|
- Status: ACTIVE (dropdown menu)
- Standardtilgang: ADMIN (dropdown menu with a '...' button to the right)
- Buttons: OK, Avbryt, Bruk



The 'Tillate tilgangsverdier' dialog box contains the following fields and controls:

- Tilgangsverdi: [Empty text box] with a 'Sett inn' button to the right.
- Tillate verdier: A list box containing 'BRUKER' and 'ADMIN' with buttons 'Slett', 'Tøm', 'Opp', and 'Ned' to the right.
- Merknader:
 - Den første verdien i listen er den laveste tilgangsverdien.
 - Kun tilgangsverdier med store bokstaver støttes.
- Buttons: OK, Avbryt, Bruk

8. TILGANG

8.1. HVOR KAN TILGANG TILDELES

- På systemet
- På brukergruppen
- På brukeren
- På applikasjonen
- På brukerdefinerte ressurser

8.2. PRIORITET

- 1. Brukeren
- 2. Gruppen
- 3. System

Når det gjelder prioritet kommer tildelte tilgang på applikasjonen også med i listen over. Er det gitt en standardtilgang på applikasjonen, vil denne overstyre gruppen. Men blir applikasjonen knyttet med en ny tilgang på brukergruppen, vil denne overstyre standardtilgang på applikasjonen.

8.3. TILGANG FLERE GRUPPER

Det er mulig for en bruker å være medlem av flere grupper. Man må da huske å sette opp denne opsjonen som Securityadministrator ***handle multiple memberships***. Vær oppmerksom på at hvis man fra før av har brukere som er medlem i flere grupper og man setter på valget "handle multiple memberships" kan man risikere at reglene endrer seg for disse. Ved dette valget vil den sterkeste tilgangen brukeren er gitt være gjeldende. Er brukeren medlem av to grupper vil tilgangen som er høyest i de to gruppene gjøre seg gjeldende.

9. GLEMT PASSORD ?

9.1. BRUKER

- Security administrator kan slette passord

Dette gjøres ved å velge mappen 'Brukere' og velge aktuell bruker. Klikk på knappen 'Egenskaper' og fjern passordet. Man kan da legge inn nytt passord på brukeren. Brukeren kan da selv endre passord til det han ønsker.

9.2. SYSTEM ADMINISTRATOR

- Kan slettes av System eller Security administrator

Dette gjøres ved først å fjerne System administrator rollen for brukeren og deretter tildele denne rollen på nytt. Nytt passord gis da for denne rollen på brukeren.

9.3. SECURITY ADMINISTRATOR

- Kan kun slettes av en annen Security administrator

Dette gjøres ved å først fjerne rollen som Security administrator, og deretter tildele denne på nytt.

10. FORSLAG TIL "HOVEDGRUPPER OG FAGGRUPPER"

Hovedprinsippet bak dette oppsettet er at en bruker blir medlem i en "hovedgruppe", samt at vedkommende **også** blir medlem i en eller flere "faggrupper", alt etter hvilke arbeidsoppgaver vedkommende har.

OBS! For at systemet skal håndtere brukere med medlemskap i **flere grupper**, må man sørge for at variabelen "Handle multiple memberships" i Security-administratoren er avkrysset.

Hovedgrupper.

Når det gjelder hovedgruppene, så er alternativene en **Supergruppe** med Delete og en **Lønn&Pers** med Query som generell tilgang. (Noen kunne kanskje ønske å ha en Supergruppe for Lønn og en for Personal, og må da sette opp en gruppe til.

Vi har også lagt inn en gruppe **Ledergruppen**, som skal dekke oppslags- og rapporteringsmuligheter for ledere, sammen med evt. registreringsoppgaver ledere måtte ha hos den enkelte kunde (eks. ferieregistrering for egne ansatte).

Hovedgrupper får f. eks. Delete-tilgang til følgende program :

Lønn&Pers m/Delete	av002per	Utforsker – Personaldata
	av011paa	Utforsker – Nærmeste pårørende
	av015kom	Utforsker – Kompetanse
	lv90-epo	Reg. av e-postadresser

Faggrupper.

Når det gjelder tilleggsmedlemskapet i en eller flere "faggrupper", åpner dette for registreringsmulighet til de oppgavene som ligger innen fagområdet. Medlemskap i faggruppen Hjemmel-Budsjett gir altså Delete-tilgang til de programmene som oppdaterer Hjemler og til kjøring av Lønnsbudsjetter, samt evt. rapporter som også foretar oppdatering i tabellene.

Dette vil gjøre det relativt enkelt å håndtere medarbeidere som skifter arbeidsoppgaver. Det er bare å melde vedkommende inn som medlem i en ny gruppe og evt. melde ut av en annen.

Faggrupper kan legges inn med generell tilgang Query. Har faggruppen None vil den ikke kunne logge på i Unique Ansatt, uten også å være medlem i en av hovedgruppene.

Vi har lagt inn noen eksempler på faggrupper. Dette skulle gi en forståelse av metoden, slik at kunden kan bygge opp sine egne grupper, for det de måtte ha behov for ut over dette forslaget. I tillegg må den enkelte kunde vurdere om faggruppene i forslaget skal ha tilgang til flere (evt. færre) applikasjoner enn det vi har lagt opp til, f.eks. i Grunndata.

Videre må kunden selv vurdere om enkelte skjermbilder bør settes ned til None-tilgang. Vi har kun gjort dette for Utforsker – Saldotrekk.

Faggrupper får Delete-tilgang til følgende	Program / Beskrivelse
Ansettelse m/Delete til	pv010sti Ansettelse – Utlysning og søkerreg. pr301bkr Ansettelse – Bekreftelsesbrev pr302inn Ansettelse – Innkallingsbrev pr303til Ansettelse – Tilbudsbrev pr304avs Ansettelse – Avslagsbrev pr305ab1 Ansettelse – Avslutte stilling pr306ab2 Ansettelse – Åpne avsl. stilling pv057med Ansettelse – Vedlikehold av media
Fraværsregistrering m/Delete til	av016fra Utforsker – Fraværsregistrering av014fer Utforsker – Ferieregistrering pr105fer Overføring av ferie pr124fer Automatisk ferieregistrering
Hjemmel-Budsjett m/Delete til	pv031hje Vedlikehold av Hjemmel (i tabell) pv029hje Vedlikehold av Hjemmel pv030hje Hjemmelsregistrering xbuds-s0 Lønnsbudsjettering lb01-est Lønnsbudsjettering – Estimering lb02-til Lønnsbudsjettering – Tillegg
LokalForhandling m/Delete til Lønnskjøring m/Del.	avl01hod Lokale forhandlinger arl05lon Overf. fra Lokale Forh.til Lønn av003ans Utforsker – Stilling m/fastlønn av004sta Utforsker – Statistikk av005pen Utforsker – Pensjon av006sal Utforsker – Saldotrekk av007not Utforsker – Notat av008var Utforsker – Var. transaksjoner av009tra Utforsker – Transaksjoner av010his Utforsker – Historikk av012yte Utforsker – Ytelser av014fer Utforsker – Ferie ajourhold av018rny Utforsker – reg. ny ansatt

Får videre Delete-tilgang til alle meny punkter under Rapport / Lønn som foretar oppdatering i tabellene.

lv07-per	Vedlikehold Lønnsperioder
xtabe-c4	Ansattliste m/overstyrt org.nr.
xtabe-c2	Endring av ansatt-data
lr98-hov	Lønnsberegning
lr99-ett	Etterberegning
xlonn-a0	Akkumulering
xlonn-c0	Ansatte med forskudd – samlet
xlonn-c1	Ansatte med forskudd – sortert

xlonn-g0	Kontant forskudd
xlonn-k3	Kontering
xlonn-o0	Overføring av var.transaksjoner
xlonn-p0	Oppdatering av hovedstilling
xarta-r1	Lønnsjustering
xtabe-y2	Kontroll still.prosent
xperi-l0	Opprykksberegning
xperi-n5	KLP-beregning
xperi-n1	SPK-oppgave (papir)
xperi-n2	SPK-oppgave (datafil)
xperi-n4	SPK-beregn. status og endr. meld.
xaars-a0	Overføring av akkumulatorverdier
xfore-b1	Skattekort retur / liste
xm-over	Overføring fra eksterne system til Ansatt

**Refusjonsbehandling
m/Delete til**

av016fra	Utforsker – Fraværsreg.
pr204fc0	Refusjonsrapporten
pv015rtv	Refusjon fra RTV
pr209fc3	Refusjon Kontering

**Variabelreg.
m/Delete til**

av008var	Utforsker – Var. transaksjoner
av102reg	Variable transaksjoner
av103per	Variable traner pr. periode
av104stv	Variable trans – std.verdier
av105kbb	Var. trans.– Kontroll bunke/bilag
av106err	Mangelfulle var. transaksjoner

Oversikt over brukerdefinerte ressurser:

Navn	Mulige verdier
rappbasis	ingen / kjore / lage
rapprans	ingen / kjore / lage
rappfrav	ingen / kjore / lage
rappferie	ingen / kjore / lage
rappkomp	ingen / kjore / lage
a-fastetranser	none / query / delete
a-lonnsoppl	none / query / delete
rolle	personal / lønn / ansatt
Forhandling	admin / bruker