

Modulet indgår som en komponent i Dialog Manager-suiten, som er en unik CRM fler-kanalsløsning, der gør virksomheder i stand til at tiltrække, bibeholde og udvikle deres kundeforhold på tværs af salgs-, service- og marketingsfunktionerne.

Security Manager, DIALOG MANAGER

SIKKERHED OMKRING DATA ADGANG

BESKRIVELSE

Security Manager sikrer gennemførelse af firmapolitik om tilgængelighed og "ejerskab" af informationer samt overholdelse af regler og bestemmelser om håndtering af data.

Ejerskab af informationer

Er et kardinalpunkt i mange virksomheder. Trenden mod selvstændige "teams", profitcentre, distrikter og regioner øger efterspørgslen for at sikre, at ejerskab og tilgængelighed af virksomhedens informationer ligeledes kan følge virksomhedens organisatoriske struktur.

Brugere og grupper

I Security Manager er der mulighed for at oprette brugere og brugergrupper for Dialog Manager. Brugere får altid tildelt et adgangsniveau, som enten "administrator" eller "bruger" - og det er kun brugere med "administrator" niveau, som har tilladelse til at bruge moduler som Design-, Security-, Batch- og Import Manager. Brugere med "bruger" som adgangsniveau er begrænset til kun at benytte Dialog Managers "daglige funktioner". Der kan oprettes et valgfrit antal brugere og grupper. Til hver gruppe kan der tilknyttes rettighederne (læse, skrive, slette, oprette).

Tilgængelighed helt ned på feltniveau

Der findes mange situationer, hvor delt ejerskab er ønskværdigt, men kun for udvalgte informationer. F.eks. ønskes stamoplysninger på en kunde gjort synligt for alle medarbejdere, mens omsætningstal, fordelt på de enkelte regioner kun gjort synligt for gruppen "Regionschefer". Udvidet egenskaber i modulet Design Manager implementerer netop denne facilitet, idet hvert eneste felt i databasen kan reagere på Security Manager og henholdsvis gøre feltet usynligt eller skrivebeskyttet.

Delt ejerskab - men kun én ansvarlig

Hvis virksomheden ønsker det, kan informationer udover ejerskab gennem brugere og grupper også påhæftes en ansvarlig. Den ansvarlige kan selvfølgelig være en fysisk person i virksomheden, men kan i høj grad også blot være en organisatorisk enhed. I én arbejdsgang flyttes informationer fra en ansvarlig til en anden og dermed tildele helt nye rettigheder på informationerne.

Automatisk tilknytning af "access" policy

For virksomheder med en eksisterende base kan det være en større opgave at gennemløbe relevante informationer og påhæfte ejerskab. Ved brug af ansvarlig tilføres hurtigt overordnet ejerskab og rettigheder på alle informationer. Herefter er det kun få informationer, som skal behandles særskilt. Ved brug af ansvarlig og en fornuftig bruger- og gruppeinddeling er det i høj grad en overkommelig opgave fuldt og helt at implementere til enhver tid gældende firmapolitik om tilgængelighed og ejerskab af information i den fulde Dialog Manager suite.



KEY BENEFITS

- ✓ Effektiv styring af eksponering af oplysninger styret enten via angivne bruger eller grupper af brugere
- ✓ Adgang til at definere valgfri antal brugere per gruppe
- ✓ Mulighed for at oprette valgfri antal grupper
- ✓ Grupperettigheder kan defineres på følgende områder:
 - Læse
 - Skrive
 - Slette
 - Oprette
- ✓ En bruger kan tilhøre mange grupper, hvor regler automatisk styrer hvilke rettigheder er overordnede og gældende i den enkelte situation
- ✓ Modulet styrer adgang så den enkelte bruger/gruppe kun har adgang til informationer med korrekt ejerskab
- ✓ Der er mulighed for indsættelse af ansvarlig på alle dimensioner
- ✓ Kaskadeopdatering af ejerskab og rettigheder
- ✓ Security Manager tilgængelig gennem DM API
- ✓ Trinvis implementering af regelsæt
- ✓ Overordnet ejerskab kan tildelse data allerede ved import:
 - Privat
 - Gruppe
 - Delt

Se FUNKTIONALITET på bagsiden



- ✓ Extended Enterprise Edition **Security Manager**, DIALOG MANAGER
- ✓ Enterprise Edition
- ✓ Professional Edition
- ✓ Small Business Edition

FUNKTIONALITET

Følgende funktionalitet er inkluderet i Security Manager:

- ◆ Valgfri antal brugere per gruppe
- ◆ Valgfri antal grupper
- ◆ Grupperettigheder: læse, skrive, slette, oprette
- ◆ En bruger kan tilhøre mange grupper
- ◆ Kun adgang til informationer med korrekt ejerskab
- ◆ Ansvarlig på alle dimensioner
- ◆ Kaskadeopdatering af ejerskab og rettigheder
- ◆ Security Manager tilgængelig gennem DM API
- ◆ Trinvis implementering af regelsæt
- ◆ Overordnet ejerskab kan tildelse data allerede ved import:
 - Privat
 - Gruppe
 - Delt

TJEKLISTE

- ✓ Sikkerhedsgrupper
- ✓ Grupperettigheder:
 - Læse
 - Skrive
 - Slette
 - Oprette
- ✓ Kaskadeopdatering
- ✓ Import ejerskab:
 - Privat
 - Gruppe
 - Delt
- ✓ DM API support