

Security Manager is part of the Dialog Manager suite, which is a unique multi-channel solution enabling you to attract, retain and grow customer relationships across traditional sale-, service- and marketing boundaries.

Security Manager, DIALOG MANAGER

SECURE DATA ACCESS

DESCRIPTION

Security Manager makes it possible to implement company policy on availability and "ownership" of information as well as to observe necessary rules and decisions regarding data handling.

Ownership of information

Is a crucial topic in many companies. The trend towards independent teams, profit centers, districts and regions helps to increase the demand for assurance that ownership and availability of company knowledge can follow the organizational structure of the company.

Users and groups

In Security Manager it is possible to create users and user groups for Dialog Manager. Users are always assigned a certain access level - either "administrator" or "user" - and only users with "administrator" access rights are allowed to use modules such as Design-, Security-, Batch- and Import Manager. Users with "user" access rights are restricted to use of Dialog Manager's "everyday functionality". An unlimited number of users and groups can be created. For each group can be attached relevant rights (read, write, delete and create).

Accessibility all the way to field level

In many situations shared data ownership is desirable - though only for selected information. For instance, a customer's Main Data is made accessible for all employees while key figures, divided into figures for each sales region, have restricted access and only made accessible for "Regional Managers". "Advanced Properties" in the Design Manager module implements exactly this facility as each of the fields in the database can respond to Security Manager and make each field invisible or read only.

Shared ownership - but only one responsible person

If the company finds it desirable, the ownership parameters can via certain users and groups be added information about responsible person. Of course, the responsible person can be a physical person in the company - but also defined as an organizational unit. In just one workflow all the information is moved from one responsible person to another and in this way assigned completely new information rights.

Automatic attachment of "access" policy

For companies with an existing database it may prove quite the labour intensive task to go through relevant information and attach ownership. By using responsible person overall information ownership and rights are rapidly attached. After this process only a limited amount of information must be handled separately. By using responsible person and a logical user- and group division it becomes a more than surmountable task to fully implement any current company policy on accessibility and ownership of information in the complete Dialog Manager suite.



KEY BENEFITS

- ✓ Efficient management of information exposure controlled either via named user or a group of users
- ✓ Access to defining unlimited number of users per group
- ✓ Possibility to create unlimited number of groups
- ✓ Group rights can be specified in the following areas:
 - Read
 - Write
 - Delete
 - Create
- ✓ A user can be attached to many groups where specific rules automatically determines which rights apply in the individual situation
- ✓ The module validates rights allowing the individual user/group only access to information with correct ownership
- ✓ Possibility to insert responsible person on all dimensions
- ✓ Cascade update of ownership and rights
- ✓ Security Manager is accessible via DM API
- ✓ Step-by-step implementation of rules
- ✓ Overall ownership can be assigned data already in connection with import:
 - Private
 - Group
 - Shared

See **FUNCTIONALITY** on back side



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

FUNCTIONALITY

The following functionality is included in Security Manager:

- ◆ Unlimited number of users per group
- ◆ Unlimited number of groups
- ◆ Group rights: Read, Write, Delete and Create
- ◆ A specific user can be attached to many groups
- ◆ Only access to information with correct ownership
- ◆ Responsible person on all dimensions
- ◆ Cascade update of ownership and rights
- ◆ Security Manager is accessible via DM API
- ◆ Step-by-step implementation of rules
- ◆ Overall ownership can be assigned data already at import:
 - Private
 - Group
 - Shared

CHECKLIST

- ✓ Security groups
- ✓ Group rights:
 - Read
 - Write
 - Delete
 - Create
- ✓ Cascade update
- ✓ Import ownership:
 - Private
 - Group
 - Shared
- ✓ DM API support