Project Realization:
User Accounts and Authorizations

SAP Business One
Release 9.0

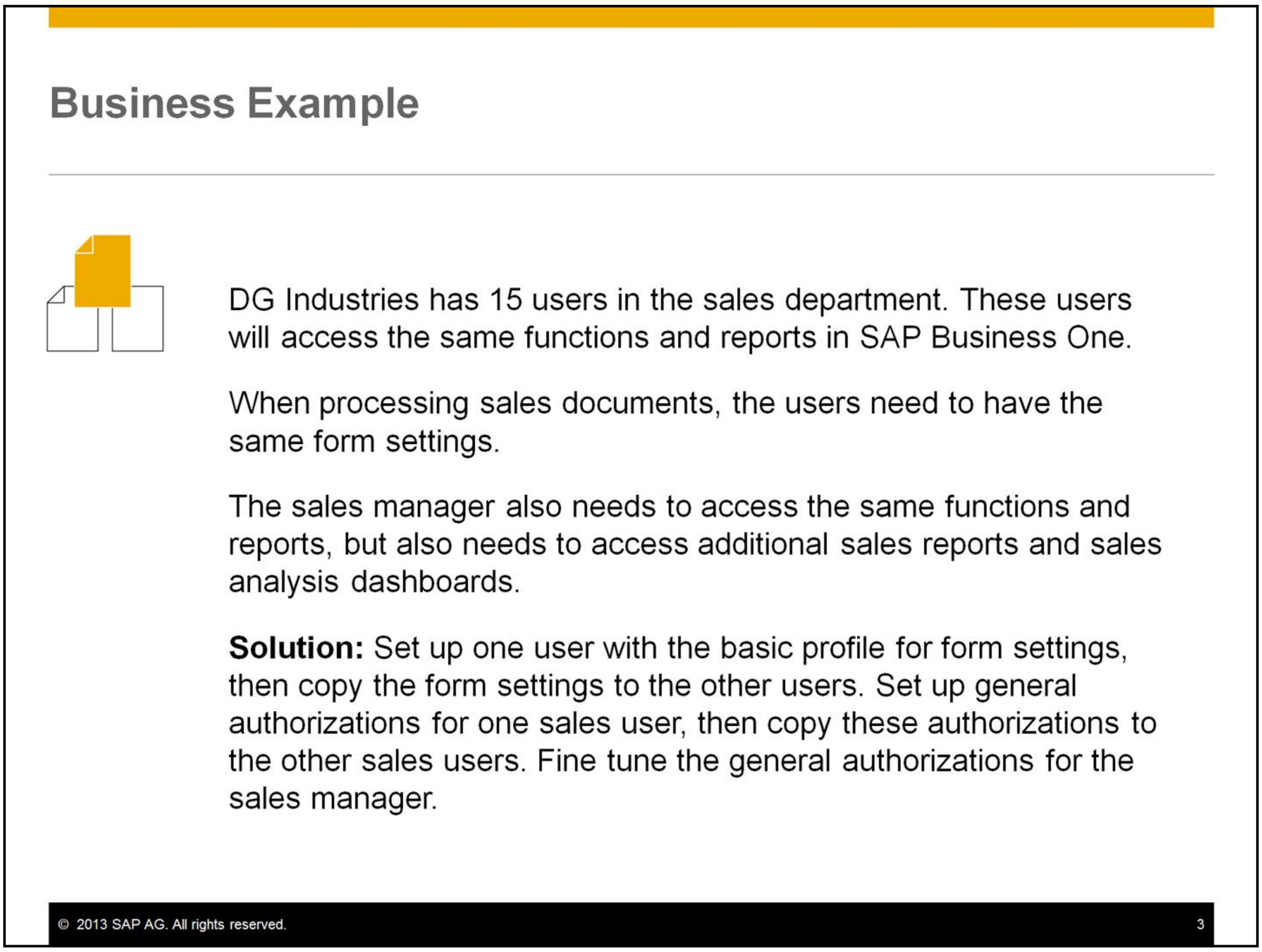
This topic covers user accounts and user authorizations.

Objectives

Objectives:

- Define accounts for users
- Grant general authorizations to functions and menus in SAP Business One
- Copy general authorizations to multiple users
- Permit or deny access to documents using data ownership authorizations

On completion of this topic, you will be able to define user accounts, and grant general authorizations to a user account so they can access functions and menus in SAP Business One.
You will also learn how to copy a set of general authorizations to multiple users, and how to limit access to documents using data ownership authorizations.



DG Industries has 15 users in the sales department. These users will access the same functions and reports in SAP Business One.

When processing sales documents, the users need to have the same form settings for documents.

The sales manager also needs to access the same functions and reports, but also needs to access additional sales reports and sales analysis dashboards.

Solution: Set up one user with the basic profile for form settings, then copy the form settings to the other users. Set up general authorizations for one sales user, then copy these authorizations to the other sales users. Fine tune the general authorizations for the sales manager.

Agenda

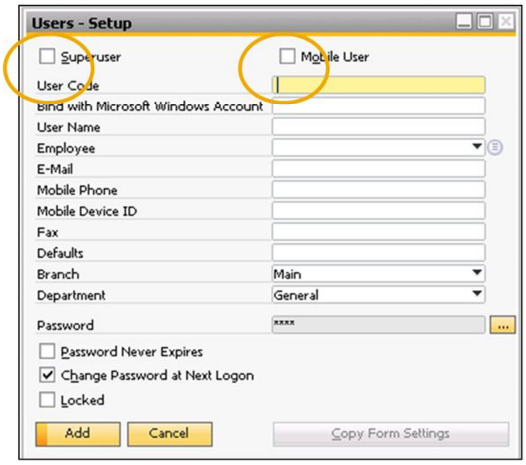
- **User Accounts**
- General Authorizations
- Document Ownership and Authorizations

The first part of this topic covers user accounts.

User Accounts

You can create user accounts from:

- ***Administration → Setup→ General → Users***
- ***Express Configuration Wizard***



Superusers

- Have all authorizations by default
- Need professional license

Users

- No authorizations by default
- Authorizations set in General and Data Ownership Authorization

 5

To login to SAP Business One, users need an account. To create user accounts, choose *Administration → Setup→ General → Users*. You can also create user accounts from the *Express Configuration Wizard*. The *User Code* must be unique and can have up to 8 characters.

There are two types of user:

- If you check the Superuser checkbox when you create a user account, the user will have full authorization to every function in SAP Business One. A super user can reset the passwords of other users and can set authorizations for other users. Obviously you should limit the number of superuser accounts.
- If you do not check the Superuser checkbox, the user by default has *no authorizations* to any system functionality. *General* and *Data Ownership Authorizations* must be set for each user.

Select the *Mobile User* checkbox to enable any user to work with a mobile device to access their company data. You should also enter the ***ID of the user's mobile device***, which they can use to access their company information.

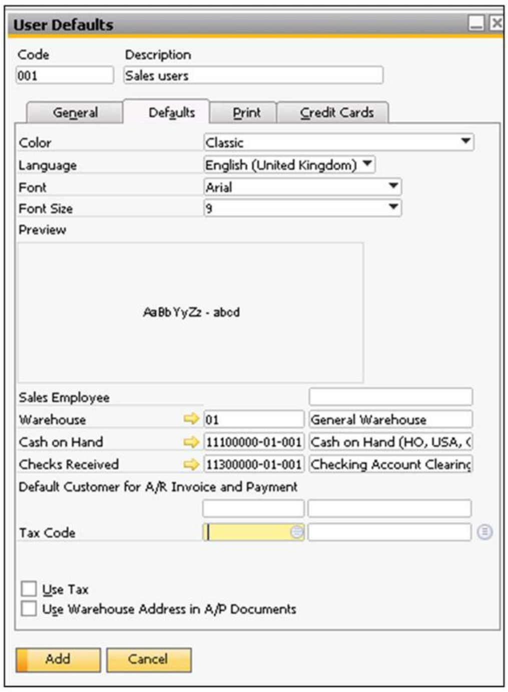
If a user fails to login successfully for the number of times specified in the *Password Administration* screen, their account will be locked (*Locked* checkbox). This is indicated in a checkbox in the user account. Only a superuser can unlock the locked user account.

User Defaults

Administration > Setup > General > User Defaults

Defaults include:

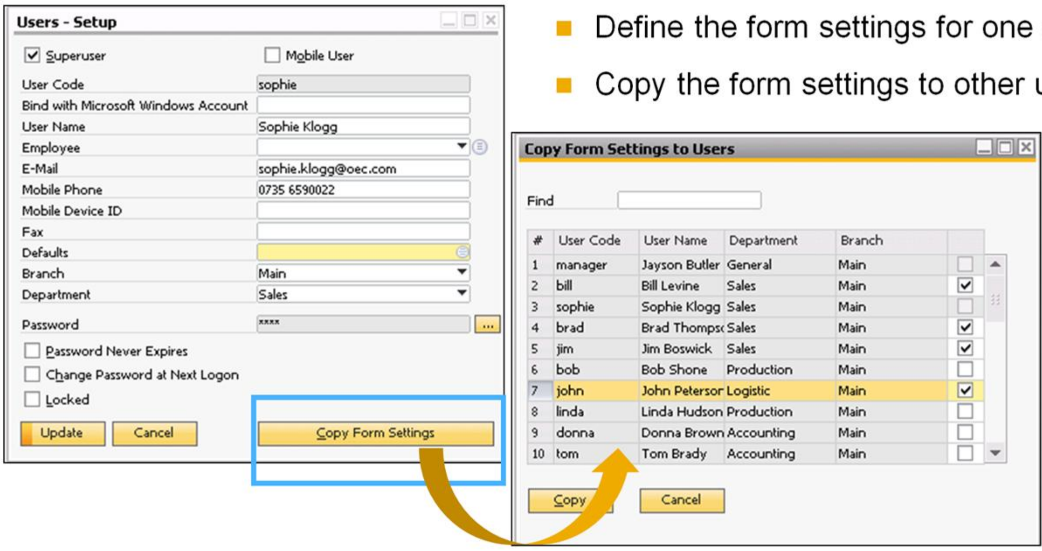
- General (Address and Communication Data)
- Default Warehouse
- G/L accounts for cash and checks
- Print Settings
- Credit Card Accounts



 6

In the User Defaults screen, you can pre-define a set of default values that are common to a group or department, such as print preferences for documents, warehouses, and certain G/L accounts used in sales. You can then assign these defaults to one or more user accounts by selecting the code for the user defaults in the user account. To set up user defaults, choose *Administration →Setup → General → User Defaults*.

Copy Form Settings



- Define the form settings for one user
- Copy the form settings to other users

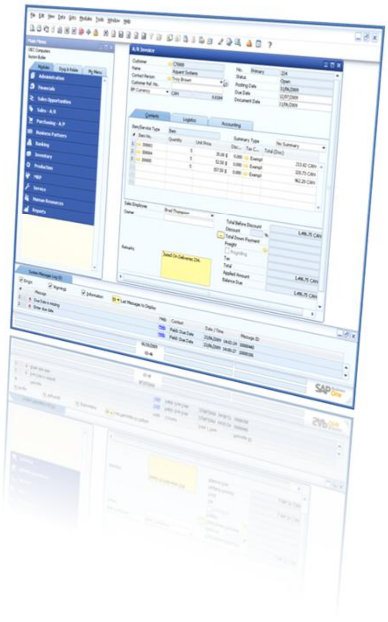
 7

Often groups of users who work in the same department have similar requirements for Form Settings in the documents they use.

You can set the required Form Settings for one user, then copy the Form Settings to other users.

This can save time during the implementation.

Demo



 8

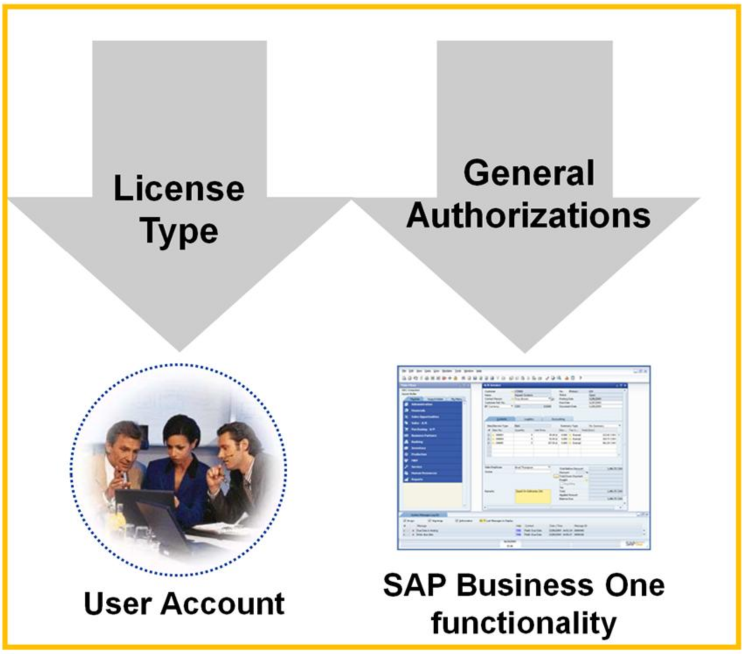
This demo will show how to define a use account for a superuser and a normal user.

Agenda

- User Accounts
- **General Authorizations**
- Document Ownership and Authorizations

The next part of this topic looks at the general authorizations needed to access functions in the system.

Authorizations - Overview



- Access to functionality is controlled through license and general authorizations
- All newly created users who are not super users have no authorizations to any SAP Business One function
- General authorizations must be set for non super users

 10

Access to the various functions in SAP Business One is controlled through a combination of license and general authorizations. These are set by user account.

- The license type assigned to a user determines which functions the user is legally contracted to use. If the user tries to access a function that is outside the scope of the license, the user will get an error generated from the license server.
- The General Authorizations granted to a user permit the user to access to the SAP Business One functions required for their job. This has nothing to do with the license but is set based on client requirements for a user’s job role. If the user has access to a function through the license, and the general authorization to the function is not set, the user will receive an authorization error when they access the function.

By default, all newly created users (except for super users) have **no authorizations** to any SAP Business One function. General Authorizations must be set for each user.

A user defined as superuser has full authorization to all SAP Business One modules and functions and it is not possible to modify the authorizations for this user.

General Authorizations

Administration → System Initialization → Authorizations → General Authorization

- Assign full access, read-only access or no access to a function or menu

 11

General authorizations can restrict if a user is allowed full access, read-only access, or no access to a function or menu.

A user designated as a superuser automatically has *Full Authorization* to all functions, but you can limit this functionality using general authorizations.

You must assign a Professional License to each superuser.

For all other users you must assign an authorization for each functional area:

- *Full Authorization* - The user can display and change data of this authorization object.
- *Read Only* - The user can only display data of this authorization object.
- *No Authorization* - The user has no access to this authorization object.

General authorizations basically follow the SAP Business One module and menu order. You can assign the same authorization to each object, or, if you expand the tree structure for the object you can assign different authorizations to the menus and windows within each area. If you do this, you see the authorization for the area becomes “Various Authorizations.”

Tip: To see the entire list of expanded general authorizations, choose the *Expand* button.

Authorizations and Roles

- Define authorizations by role for representative user, then copy to other users

 12

General authorizations are set user-by-user; however, if the customer has groups of users who perform the same tasks, the fastest way to assign general authorizations is by role.

One way of doing this is to present the various SAP Business One functions (modules and menus) to a nominated representative user for each role. This person then marks the functions that they use.

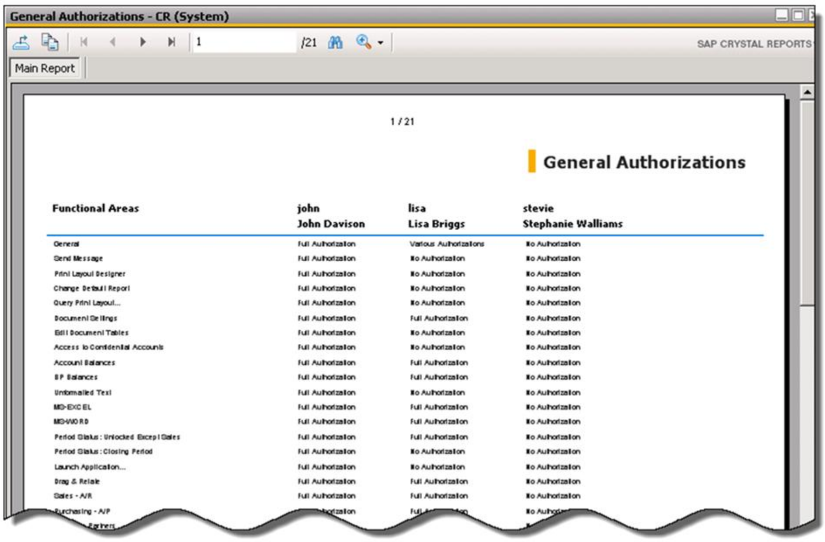
Next, create a user account for the representative user and assign the correct license type to this user. Test to make sure that the combination of license and general authorizations provides access to the required functionality for the role.

You can then copy this set of authorizations from one user to another user, from the general authorizations window. Select the source user name in the authorizations window, then drag the source user name over the target user name.

In the AIP materials you can use the Business Process Master List (BPML) tool to help you define customized roles according to SAP Business One functions.

Authorizations Report

- Print report of authorizations for selected users
- Export list of authorizations to Microsoft Excel



 13

After you have set the general authorizations you can print a report with a full list of authorizations for up to four selected users.

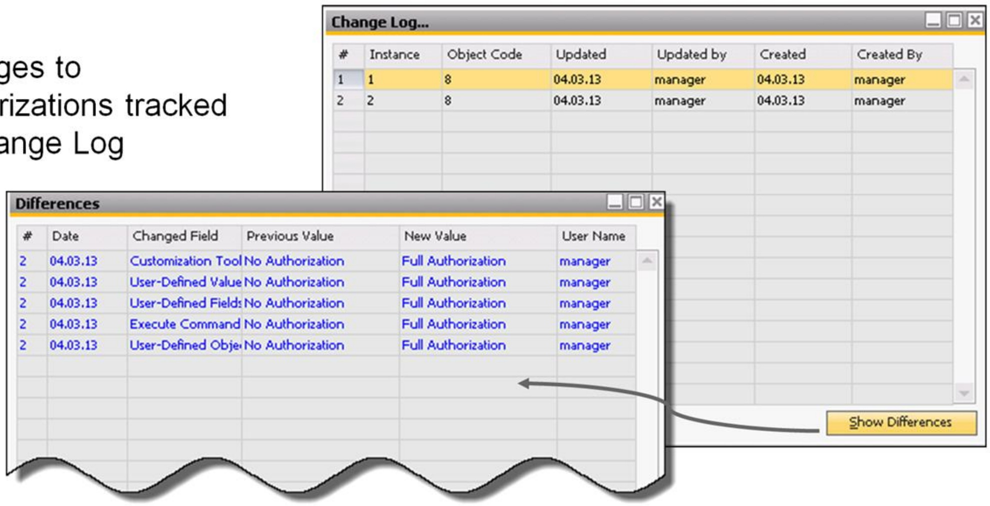
Additionally, you can export the complete list of authorizations to Microsoft Excel or as a PDF file. This allows you to review each authorization offline with the client, and make any required adjustments.

To see the effect of each general authorization, refer to the how-to guide *How to Define Authorizations*.

Tracking Changes

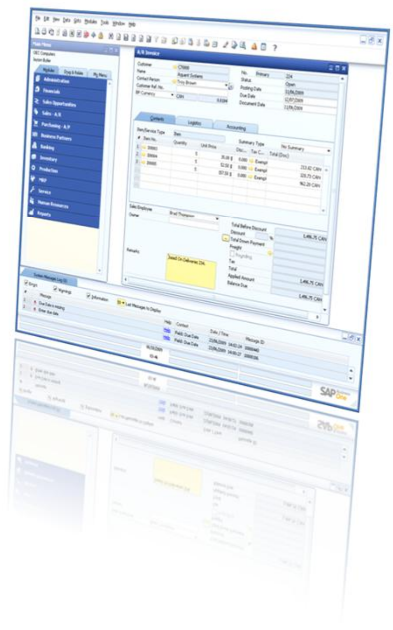
Tools > Show History

- Changes to authorizations tracked in Change Log



Changes to authorizations are tracked in the change log. To open the change log, make sure the General Authorizations window is active, then choose *Tools > Show History*.

Demo



 15

This demo will show you how to set general authorizations for a user, and copy those authorizations to other users with a similar role.

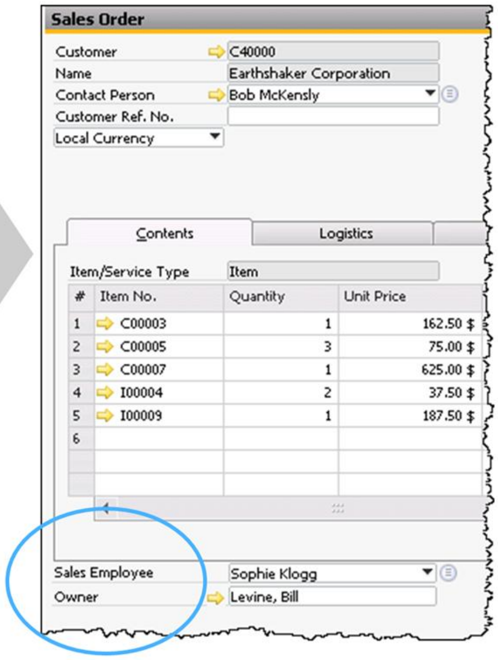
Agenda

- User Accounts
- General Authorizations
- **Document Ownership and Authorizations**

The last part of this topic looks at document ownership and document ownership authorizations.

Ownership of Documents

- Document can be optionally linked to a designated sales or purchasing employee
- Document can have a designated owner that can be different to the sales employee or buyer, or to the business partner contact person



 17

Every document can be optionally linked to a designated sales or purchasing employee. And every document can have a designated owner. The owner can be a different user from the sales or purchasing employee, and from the contact person for the business partner.

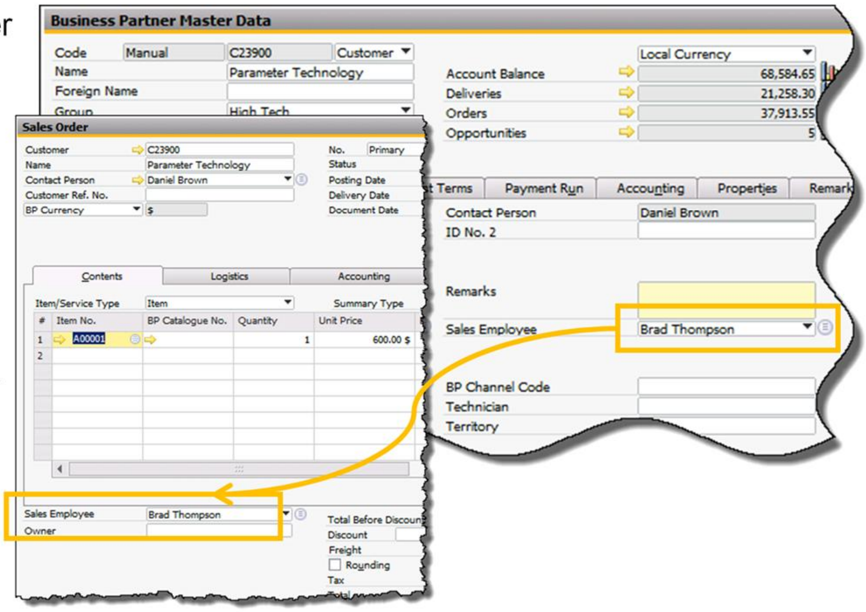
So how can you designate the sales employee / buyer or the owner for a document?

Sales Employees/Buyers

Administration > Setup >General > Sales Employees/Buyers

Sales employee / buyer defaults in from business partner master data

1. Define sales employees and buyers in system
2. Assign sales employee or buyer to business partner master data
3. Sales employee or buyer selected in documents for the business partner



The sales employee / buyer that is linked to a document defaults in from the business partner master data.

First you need to define the sales employees and buyers in the system. Choose *Administration > Setup >General > Sales Employees/Buyers.*

Once setup, you can now assign the responsible sales employee or buyer to relevant business partner master data records.

The name of the sales employee or buyer will be automatically selected in all marketing documents created for the business partner.

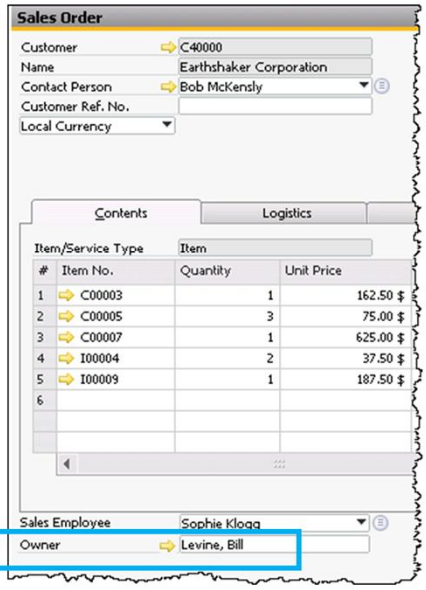
Of course the sales employee or buyer name can be changed in an individual document if required.

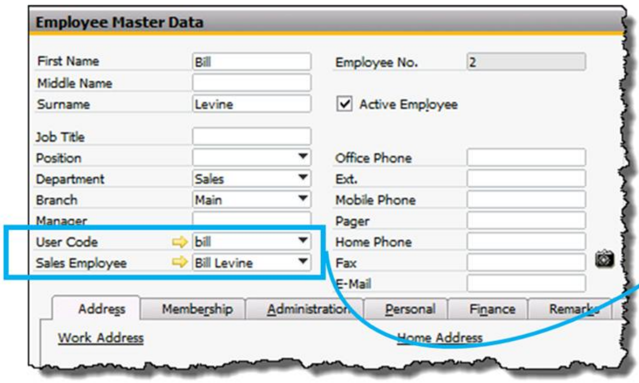
Assigning the relevant sales employee / buyer to the respective business partners, and later to each sales or purchasing document, enables the customer to do the following:

- Generate sales analysis and purchasing analysis reports by sales employee or buyer
- Assess the sales / purchasing volume achieved by each sales employee / buyer

Document Owner

- The owner is normally the user who creates the document
- However, if there is a designated sales employee or buyer for a document, and the sales employee / buyer is linked to an employee master data record, then the sales employee / buyer becomes the owner of the document



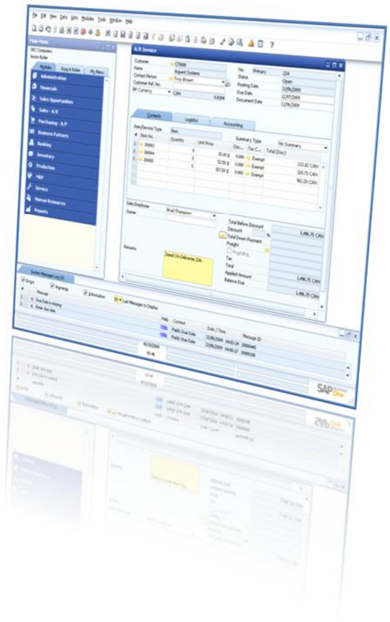


 19

The owner of a document is normally the user who creates the document; however, if there is a designated sales employee or buyer for the business partner, and the sales employee or buyer is linked to an employee master data record, then the sales employee or buyer becomes the default owner.

In the example, the user Sophie Klogg has created a sales order for Earthshaker Corporation. Bill Levine is set as the designated sales employee for this customer, and since Bill Levine also has a linked employee master data record, then Bill Levine automatically becomes the owner.

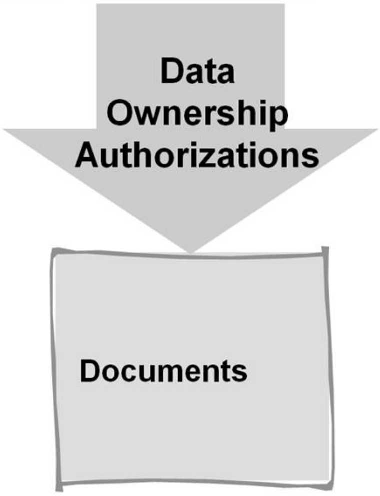
Demo

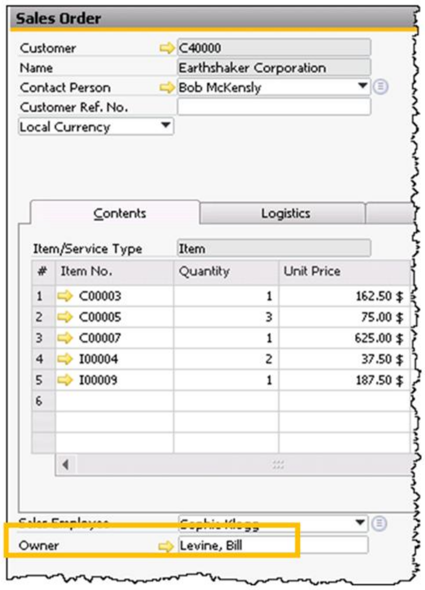


In this demo, you will see how to assign a sales employee/buyer and an owner to a document.

Data Ownership Authorizations

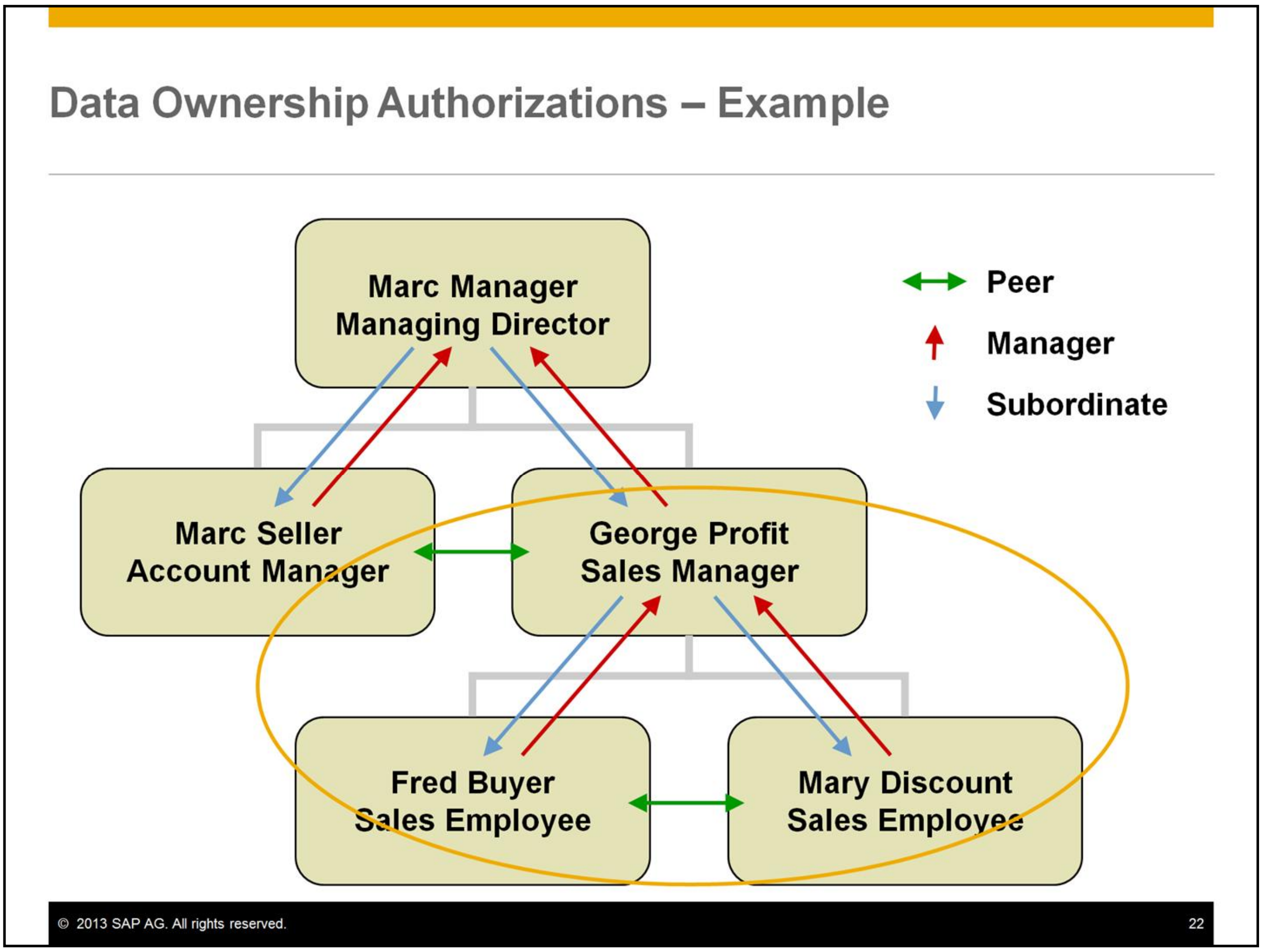
- Who else should be allowed to view or change a document or document rows?
- What is the person's relationship to the owner of the document?





The owner of a document is the basis for another type of authorization – Data Ownership Authorizations.

Using data ownership authorizations, you can permit another person access to a document and even to the rows in a document based upon the person's relationship to the *owner*. This is mostly relevant for departments such as sales and purchasing where there might be a need to restrict access to documents from within a department.



Here is a simple example. We can set up employee master data records to model this organization, for the purposes of data ownership.

In the master data for the sales employees Fred Buyer and Mary Discount, we select George Profit as the manager. We also need to create a master data record for the manager.

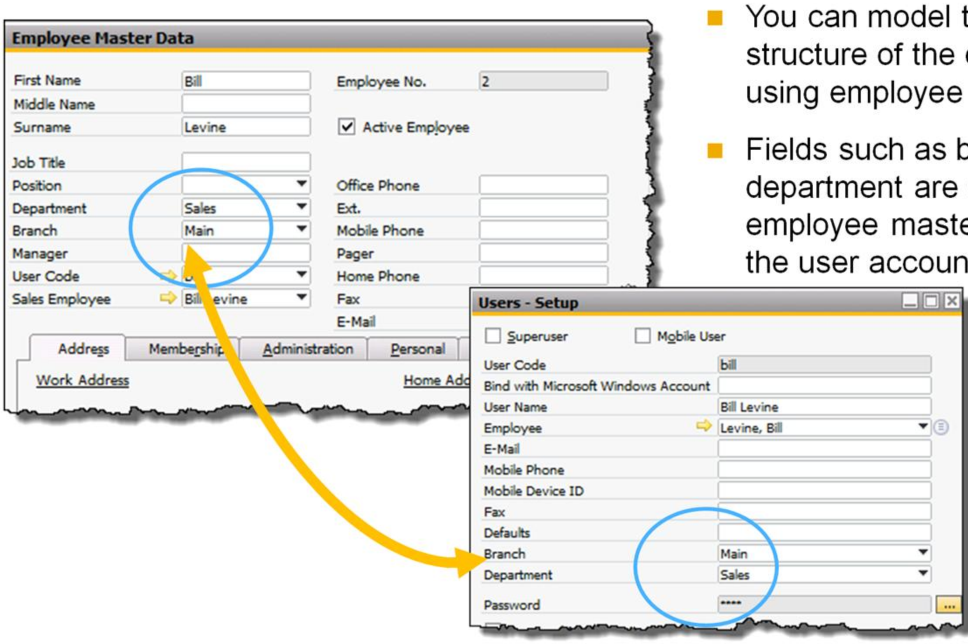
Also in the master data we select the same department for all three employees, thus linking them using both the department and the management structure.

For data ownership authorization purposes, we can define the relationships as:

- Peer: The user can access documents *owned* by a colleague at the same level in the hierarchy.
- Manager: The user can access documents *owned* by his or her direct manager.
- Subordinate: The user can access documents *owned* by any of his or her direct subordinates.

Employee Master Data

Human Resources > Employee Master Data



- You can model the reporting structure of the organization using employee master data
- Fields such as branch and department are common to employee master data and the user account

 23

You can use employee master data to model the organization of a company. To define employee master data records, choose *Human Resources > Employee Master Data*.

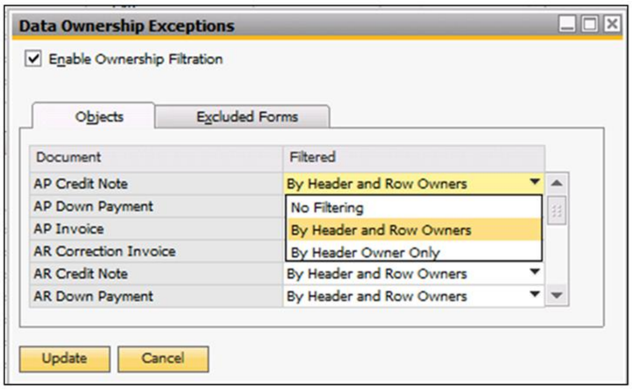
In the master data, you can specify information about an employee, such the department, manager, and role within the organization. You can also record personal information for the employee, and some HR data.

Many fields are common between the employee master data and the user account. When you add an employee master data record, you can optionally generate a user account, if one does not exist. If a user account exists, you can have common fields copied from the master data to the user account.

Enabling Data Ownership Authorizations

Administration > System Initialization > Authorizations > Data Ownership Exceptions

- Enable / disable data ownership system wide
- Once set, users have restricted access to documents and sales opportunities, and even to document rows, based on a defined relationship with the document owner
- You can bypass filtering on a document by document basis



 24

Data ownership can be enabled or disabled system wide using the *Data Ownership Exceptions* screen. Once set, users will have restricted access to documents and sales opportunities, and even to document rows, based on a *defined relationship* with the document owner.

In this window, you can also select which objects are subject to data authorization restrictions, either fully or partially. If you select *No Filtering*, for an object, then data ownership is not active for the object. In the case that a document or sales opportunity has no owner defaulted in, then any user can access it as if no data ownership is in place.

Assigning Data Ownership Authorizations

Administration → System Initialization → Authorizations → Data Ownership Authorizations

- After enabling data ownership filtration, the next step is to define the permissions for each user for each relationship, by document

User: Fred Buyer

Document	Peer	Manager	Subordinate	Department	Branch	Team
Sales Order	Full	None	None	Read Only	None	Full
A/R Invoice						
Purchase Order						
. . .						

Fred Buyer can view (and optionally update) sales orders owner by peers and team colleagues.

After enabling data ownership filtration, the next step is to define the permissions for each user, in the *Data Ownership Authorizations* screen.

A user can access a document as long as he or she has a defined relationship with the owner of the document and has been granted either *Read Only* or *Full* for the data ownership permission for that relationship. The full range of possible relationships is:

By reporting line:

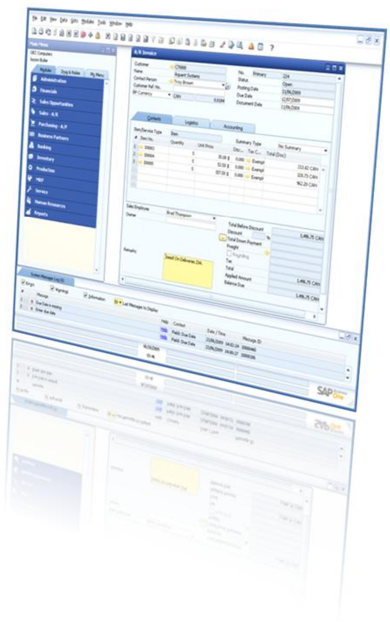
- Peer: The user can access documents owned by a colleague on the same level in the hierarchy.
- Manager: The user can access documents owned by his or her direct manager.
- Subordinate: The user can access documents owned by any of his or her direct subordinates.

By organizational line:

- Department: The user can access documents owned by a member of the same department.
- Branch: The user can access documents owned by a member of the same branch.
- Team: The user can access documents owned by a member of the same team.

In the example, the user Fred Buyer can view (and optionally update) sales orders owner by his peers and colleagues in the same team. Fred has no access to sales orders owned by his manager or by users in his branch. He can only view sales orders owned by users in the same department.

Demo



 26

In this demo, you will see how to define data ownership authorizations to documents.

Key Points

Key points from this topic:

- There are two types of user account:
  - A superuser has by default full authorization to every function and needs a Professional license
  - Non superusers have no authorization to any function and you need to grant general authorizations to each user
- The easiest way to grant authorizations is by role, and copy the authorizations from one user to other users
- You can designate users as a sales employees or buyers, and can assign a default sales employee or buyer for a business partner
- Employee master data enables you to define an organizational structure with reporting lines. Employee master data is required for data ownership authorizations
- If the business partner has a designated sales employee or buyer, linked to employee master data, the sales employee or buyer is the owner of documents created for the business partner.

Here are some key points to take away from this session.

- There are two types of user account. If you check the Superuser checkbox when you create a user account, the user will have full authorization to every function in SAP Business One. Super users need a Professional license. If you do not check the Superuser checkbox, the user by default has *no authorizations* to any function and you need to grant general authorizations to each user.
- The easiest way to grant general authorizations is by role, and you can copy the authorizations from one user to other users with similar roles.
- You can designate users as sales employees or buyers. Once setup, you can assign the responsible sales employee or buyer as a default for a business partner.
- You can also define employee master data. This enables you to define an organizational structure with reporting lines. Employee master data is required for data ownership authorizations. These authorizations permit or deny another user access to a document based upon the user’s relationship to the owner of the document.
- If the business partner has a designated sales employee or buyer, and the sales employee / buyer is linked to employee master data, then the sales employee or buyer is by default the owner of documents created for the business partner.

Thanks!

You have completed the topic for

user accounts and authorizations

in SAP Business One.

Thank you for your time!

You have completed the topic for user accounts and authorizations in SAP Business One. Thank you for your time!