



T-SYSTEMS MULTIMEDIA SOLUTIONS

# ADMINISTRATION MANUAL

DOCULIFE DESKTOP 5.6

DATE: 16.03.2015

T · Systems ·

doculife®

© Document Future AG 03/2015

Document Future AG holds the copyright to this documentation. No part of this documentation may be reproduced, regardless of the method used (e.g., printing, photocopy, microfilm), without previous written consent from Document Future AG. No part of this documentation may be processed, copied, or distributed with the use of electronic systems without previous written consent from Document Future AG.

<http://www.documentfuture.com>

# Table of contents

<b>1</b>	<b>Introduction</b>	<b>5</b>
<b>2</b>	<b>Formatting and layout used throughout this documentation</b>	<b>6</b>
<b>3</b>	<b>General security information</b>	<b>7</b>
3.1	Anti-virus protection	7
3.2	Saving passwords	7
3.3	Using mobile devices	7
<b>4</b>	<b>Administrator tasks</b>	<b>8</b>
<b>5</b>	<b>Terms and definitions</b>	<b>9</b>
5.1	Tenant	9
5.2	Solution	9
5.3	Files	10
5.4	Register	10
5.5	Document	10
<b>6</b>	<b>Open System Configuration</b>	<b>11</b>
6.1	Overview	11
6.2	Templates and User Management	11
6.3	Common update settings	13
6.4	Display and manage add-ins	13
<b>7</b>	<b>Permissions concept</b>	<b>14</b>
7.1	Overview of the permissions concept	14
7.2	Types of access permissions	15
7.3	Users	16
7.4	Groups	16
<b>8</b>	<b>Managing users</b>	<b>18</b>
8.1	Requirement	18
8.2	Adding users	18
8.3	User types	22
8.4	Guidelines for strong passwords	22
8.5	Assigning management information	22
8.6	Managing users	24
8.6.1	Resetting passwords	24
8.6.2	Changing the groups for a user	26
8.6.3	Sharing scanning activation files	27
8.6.4	Providing an additional user account for a user	28
8.6.5	Editing user information	30
8.7	Closing a user account	31
8.7.1	When to close an account	31
8.7.2	Deactivating a user account	31
8.7.3	Reactivating a user account	33
8.7.4	Deleting a user account	34
8.8	Overview of technical users	35
8.9	Displaying technical users	36
<b>9</b>	<b>Managing groups</b>	<b>37</b>
9.1	Overview	37
9.2	Adding a user group	37
9.3	Showing the members of a group	40
9.4	Displaying group memberships	40
9.5	Groups used to provide access permissions	41

9.6	Technical groups .....	42
9.7	Deleting groups .....	44
<b>10</b>	<b>SECplus / SECmezzanine key administration .....</b>	<b>45</b>
10.1	Overview .....	45
10.2	Locking tenants .....	45
10.3	Granting permissions for locking a tenant .....	47
10.4	Changing keys .....	48
<b>11</b>	<b>Inboxes .....</b>	<b>51</b>
11.1	Overview .....	51
11.2	Personal inboxes .....	51
11.3	Group inboxes .....	51
11.4	Managing inboxes .....	52
11.4.1	Adding inboxes to the inbox overview .....	52
11.4.2	Opening and working with a user's inbox .....	53
11.4.3	Group inbox .....	54
<b>12</b>	<b>Finding documents .....</b>	<b>57</b>
<b>13</b>	<b>Solution administration .....</b>	<b>58</b>
13.1	Overview .....	58
13.2	Saving templates in the filesystem .....	58
13.3	Creating searches .....	60
13.3.1	Creating searches .....	60
13.3.2	Making available to all users .....	60
13.4	Choice lists .....	61
13.4.1	Overview .....	61
13.4.2	Opening a choice list .....	61
13.4.3	Changing the label for an index value .....	62
13.4.4	Adding index values .....	63
13.4.5	Editing and adding nodes .....	64
13.4.6	Deleting index values and nodes .....	66
13.5	Updating templates .....	67
13.6	Solution updates .....	68
13.7	Saving and publishing changes .....	70
13.8	Revoking published templates .....	72
13.9	Feature set .....	72
13.9.1	Feature set overview .....	72
13.9.2	Adding a feature set .....	72
13.9.3	Feature set .....	73
<b>14</b>	<b>Audit .....</b>	<b>74</b>
14.1	Overview .....	74
14.2	Searching for events .....	75
14.3	Calls for events .....	76
<b>15</b>	<b>Administration rights .....</b>	<b>79</b>
15.1	Administrator .....	79
15.2	Granting management permissions .....	79
<b>16</b>	<b>Index .....</b>	<b>81</b>

# 1 Introduction

This documentation describes how to manage a doculife tenant with Desktop Version 5.6. It is intended for end-user administrators.

In order to be able to understand this documentation, the user must be familiar with the use of doculife and with the user manual for doculife Desktop.

---

**Please note:**

The administrator functions that are available will depend on the solution being used and the extent of your administrator rights. If you have any questions, please contact doculife Support.

---

All the examples and screenshots in this manual are based on the default configuration for doculife and therefore may not be an exact match for your actual setup.

For additional information on structures, metadata, the permissions concept, and custom-ordered parameter configurations, please refer to the solution descriptions for the solutions you are using.

## 2 Formatting and layout used throughout this documentation

This section goes over the most important formatting and layout choices used throughout the online help. The purpose of these choices is to enable you to get started quickly.

### Buttons, icons, menu commands, keys, window titles, messages, and prompts

These are all shown in **bold**.

In addition, key names are written in uppercase letters (e.g., **ENTER**).

### Notes

Notes contain additional information and are indicated as follows:

---

**Please note:**

This is a note.

---

### Definitions

Definitions for terms and structure specifications are indicated as follows:

The definition for the term “print server” would be provided here.

### Tip

Useful shortcuts, additional options, and special settings are indicated as follows:

**Tip:**

This is a tip.

### Important

“Important:” is used to point out information that is important for the process or workflow in question or for ensuring that an instruction can be carried out.

### Examples

Examples of individual functions are indicated as follows:

**Example:**

This is an example.

### Instructions / step-by-step instructions

When there are multiple instructions / step-by-step instructions, they will be numbered in ascending order.

Instructions that only require one single action are indicated with the ► arrow icon.

## 3 General security information

This section contains general security information concerning the use of doculife.

Make sure to read it carefully.

### 3.1 Anti-virus protection

doculife does not provide any additional anti-virus protection.

This means that documents and e-mails transferred to doculife will not be checked for malware in doculife.

Make sure to check all documents and e-mails for malicious code on the computer before storing them in doculife.

---

**Attention: risk of data loss**

Use an anti-virus product that monitors your data, e-mail, and Internet communications and protects your computer from attacks.

---

### 3.2 Saving passwords

Due to security reasons, users have to enter their password every time they log in to their doculife account (i.e., connect to the system).

It is possible to configure the system in such a way that users will be able to save their password for a tenant.

---

**Attention: risk of misuse of data**

Saving login information can enable unauthorized users to access your data. Please make absolutely sure that saving login information is allowed by your company's security policies before doing so.

---

### 3.3 Using mobile devices

Mobile devices are more vulnerable to malware and spyware attacks. Users are responsible for the security of their own devices.

---

**Attention: risk posed by unauthorized data mining and access**

Make sure to only load apps from trustworthy sources on your device. Use appropriate software designed to protect you from spyware and similar attacks.

---

## 4 Administrator tasks

doculife tenants are managed by the **Administrator** user. Administrators activate doculife tenants and load the desired solution.

After setup, managing a doculife tenant includes:

- Creating and managing users and user groups
- Creating and managing group inboxes
- Maintaining choice lists and templates
- Loading new solutions and updating existing solutions

---

**Please note:**

Your account must be associated with the corresponding tenant in order for you to be able to use the various administrator permissions.

---



## 5 Terms and definitions

### 5.1 Tenant

In doculife, tenants are units that are organizationally and technically independent of each other.

---

**Please note:**

Throughout this document, the term “tenant” is used the same way as it is used in IT. It describes how an organizational unit is mapped in doculife.

---

In doculife, the processing of files, registers, and documents for the individual tenants is kept strictly separate, as is the data storage for each tenant. Moreover, all access is based on tenant-specific access permissions.

The following applies when it comes to tenants:

- The user interfaces, structures, search templates, search result lists, choice lists, and index values for a tenant’s files, registers, and documents are independent of other tenants
- A tenant’s user and permissions management is independent of other tenants
- Languages can be selected in a tenant-specific and user-specific way
- One or more solutions can be run for a single tenant
- Specific recognition solutions can be optionally integrated for a tenant

### 5.2 Solution

A solution is a DMS application installed specifically for a tenant.

The following applies to solutions:

- One or more solutions can be run for a single tenant independently of each other
- Each solution will feature its own permissions scheme
- File, register, and document index fields; search templates; search result lists; and choice lists can be individually modified and expanded for each solution.
- In each of the solutions for a tenant, the repository can be independently structured with files, registers, and documents independently of the tenant’s other solutions

The administrator is the one who selects and loads solutions the first time a tenant is activated.

---

**Please note:**

For more information on loading solutions, please refer to the “Initial activation” section in the doculife – Getting started documentation.

---

Loaded solutions can be modified by:

- Having the administrator provide new searches, templates, and choice list contents
- Updating the solution with custom modifications made and provided by the solution’s vendor

### 5.3 Files

In solutions installed for a doculife tenant, documents are stored in files (folders), which can be subdivided into registers. This means that documents with various formats (e.g., PDF, Office, e-mails) can be grouped together and stored in a file and its registers.

Documents can be stored in files either without a specific structure or following a specific storage structure. In fact, registers can be used to create as many hierarchical storage structures as necessary in a file.

Files have index fields, which can be used to store index values (metadata) that describe the files.

Files can be assigned to a variety of file types. Each file type has a series of custom index fields that depend on the intended use of the corresponding file within the business.

Any number of file types can be used in a solution.

### 5.4 Register

Registers (subfolders) are used to subdivide files in order to store documents that logically belong together (in terms of format and/or content) in their own separate location. In addition, registers can contain their own registers.

Registers have index fields that can be used to store index values (metadata) describing the corresponding register.

Registers can be assigned to various register types. Each register type has a series of custom index fields that depend on the register's intended use.

Any number of register types can be used in a solution.

### 5.5 Document

A document is an individual information object stored for a specific doculife tenant. doculife supports both digitized objects and objects originally created in an electronic format.

Documents have index fields that can be used to store index values (metadata) describing the corresponding document.

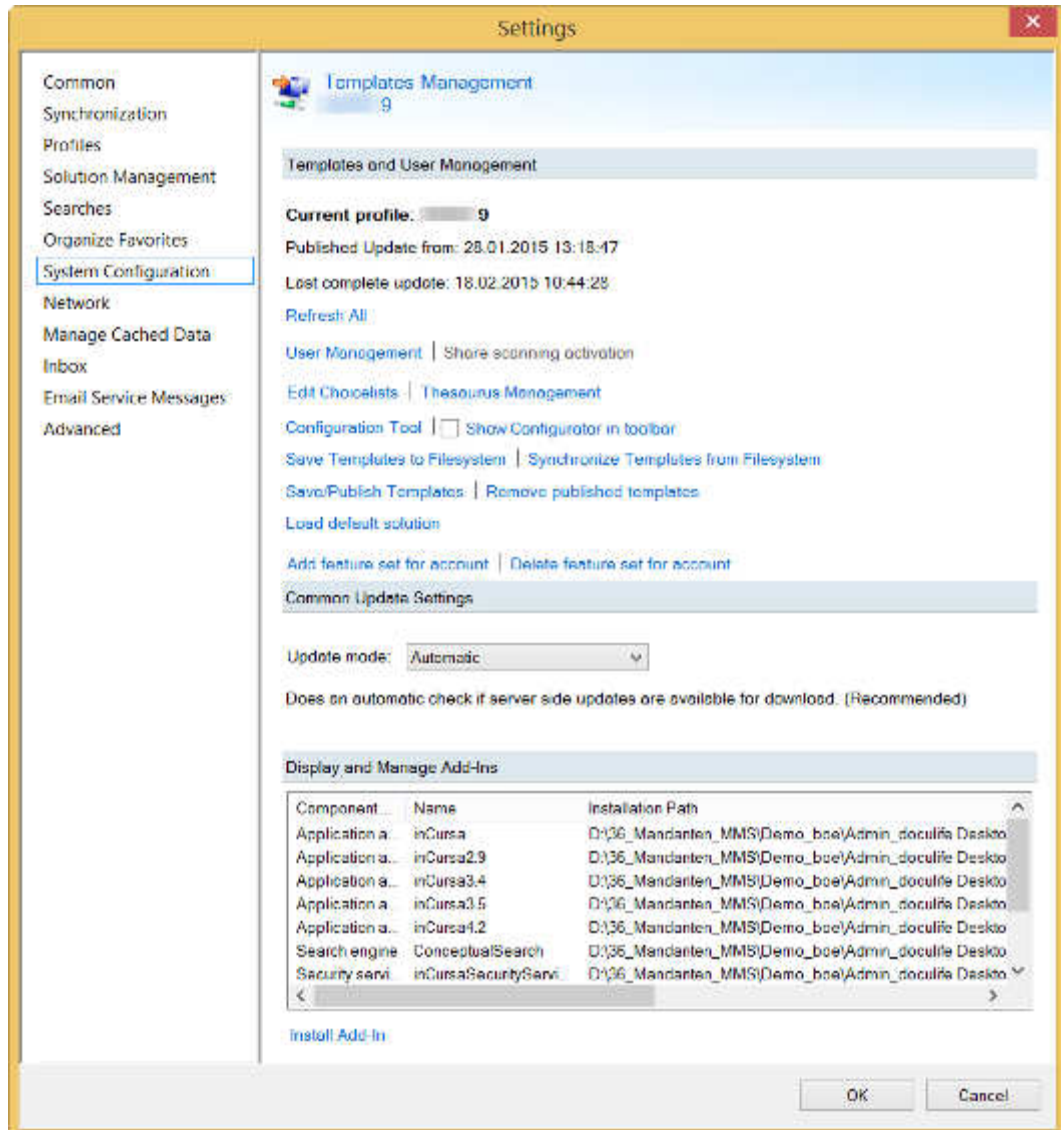
In order to specify its type in greater detail, a document can be assigned to a specific document type. This assignment will make it possible to use index fields specific to the document type.

Any number of document types can be used in a solution.

## 6 Open System Configuration

### 6.1 Overview

The functions available for managing users, groups, and solutions can be accessed through **Settings, System Configuration**.



### 6.2 Templates and User Management

#### Current profile

- The name of the tenant / profile with which you are currently logged in
- Published Update from: The date and time of the latest published template update
- Last complete update: The date and time of the most recent complete update

#### Synchronize to Server

Function for manually updating all templates and choice lists.

---

**Please note:**

It is recommended to have the program run updates automatically and to manually synchronize the templates and choice lists only when necessary.

---

**User Management**

Opens the menu for managing users and groups.

**Share scanning activation**

Generates the scanning key required in order to activate the direct scanning integration feature.

**Editing choice lists**

Opens the dialog box used to edit choice lists.

**Thesaurus Management**

Opens a dialog box that can be used to edit and manage the thesaurus (optionally available).

**Configuration Tool**

Opens a configurator (optionally available) for editing templates.

**Show Configurator in toolbar**

Adds an icon to the toolbar that can be used to start the configurator (optionally available).

**Save Templates to Filesystem**

Opens the dialog box used to save templates locally.

**Synchronize Templates from Filesystem**

Opens a dialog box that can be used to synchronize template changes and additions made locally with templates being used actively.

**Save/Publish Templates**

Opens a dialog box that can be used to save and publish edited templates.

**Remove published templates**

Undoes the last template publication.

**Load solution**

Opens a dialog box that can be used to load a solution from the filesystem.

**Add feature set for account**

Function for loading a tenant-specific configuration. This configuration will provide tenant parameter configurations that are independent of the solutions being used.

**Delete feature set for account**

Function for deleting a tenant-specific configuration.

## 6.3 Common update settings

### Update mode

Every time Desktop starts, the program will check whether there are any new or changed templates on the server that need to be transferred and used.

The following options are available:

- **Automatic:** When starting Desktop, the program will automatically check whether there are any new templates on the server and load them. This is the recommended setting.
- **Always:** The program will check all the settings on the server at cyclic intervals. This may take a few minutes.
- **Manual:** The program will not check automatically whether there are any new or changed templates on the server. If you select this option, updates will have to be carried out manually. Recommended for experienced users only.

## 6.4 Display and manage add-ins

This list shows the add-ins that have been installed.

To install an add-in, click on **Install Add-In** and select the add-in (\*.AddIn.zip) in the Windows File Explorer.

To uninstall an add-in, **right-click** on it and then click on **Uninstall**.

---

**Please note:**

Add-ins required in order for Desktop to work properly cannot be uninstalled.

---

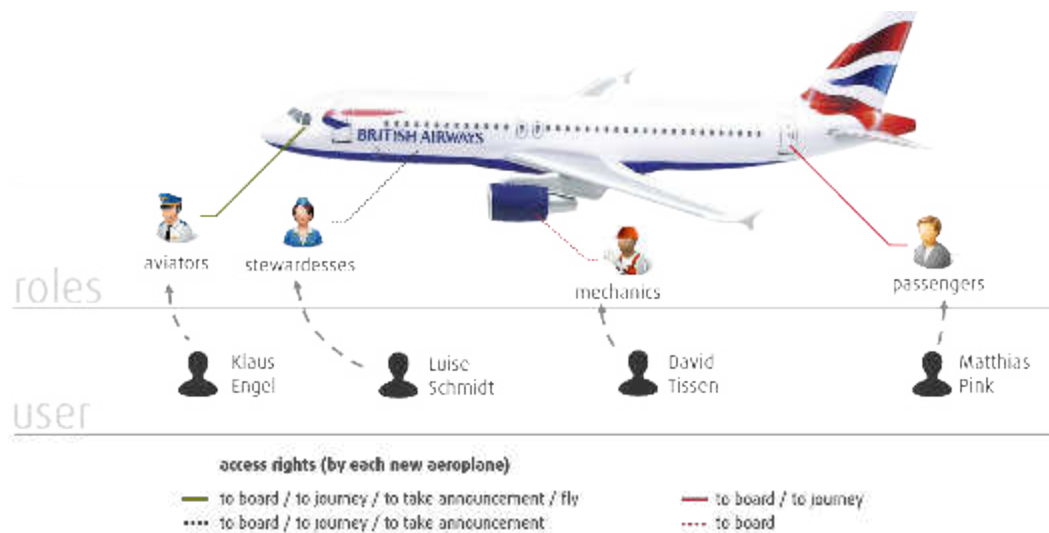
## 7 Permissions concept

### 7.1 Overview of the permissions concept

doculife features an easy-to-understand, fine-grained, role-based permissions concept for files, registers, and documents that is designed with real-life applications in mind. In it, data access and editing permissions are defined in detail using a permissions scheme and are then managed at the group level.

#### Data access and editing permissions

Access permissions for editing files, registers, and documents (data access and editing permissions) are grouped together and provided for user groups (roles). Users are assigned to these groups based on their responsibilities and authorization levels and are assigned permissions (data access and editing permissions) for their work in the DMS.



#### Confidentiality levels

The required confidentiality levels and the extent of the data access and editing permissions for a user group are determined based on the specific existing security requirements for the documents that will be stored in doculife. The following are determined during the process:

- Who is allowed to view which files and documents
- Who is allowed to edit these files and documents and to what extent they are allowed to do so

The following confidentiality levels will be defined in a doculife standard solution by default:

- Confidential: For confidential files and documents
- Default: For day-to-day business files and documents
- Public: For generally accessible files and documents
- Only me: For files and documents to which only you, as the author, will have access at first, but for which you can “unlock” access for other users in a targeted manner.

#### Permissions scheme

The system-side relationships between the defined confidentiality levels for files, registers, and documents and the various user groups are referred to as a “permissions scheme.” A per-

missions scheme represents a solution's permissions system in summarized form and is the basis for managing users and groups.

## 7.2 Types of access permissions

The following types of access permissions are available in doculife:

Permission	Description
Create (C)	Creating files
Read (R)	Searching, browsing (viewing contents), viewing properties, viewing attachments, showing permissions, viewing document contents, showing document versions
Author Document (A)	Creating documents
Write (W)	Editing properties, creating registers, adding documents and links, checking documents out/in, editing document contents
Delete (D)	Deleting files, removing links, removing / deleting documents
Security (S)	Changing permissions, taking over ownership

The permissions assigned to a group are grouped together and shown as follows in an object's properties (**Properties, Access Rights, Access Rights** column):

Access permission	Description of permissions
Read access	Searching, browsing (viewing contents), viewing properties, viewing attachments, showing permissions, viewing document contents, showing document versions
Read/write access	<b>In addition to the rights that come with read access:</b> Editing items, changing item properties, checking documents in and out, creating and deleting links, creating new items
Read / Write / Delete	<b>In addition to the rights that come with read/write access:</b> Delete Items
Full access	<b>In addition to the rights that come with read/write/delete access:</b> Setting and modifying access permissions, taking over ownership permissions for an item

## 7.3 Users

doculife distinguishes between:

- Business users
- Technical users

### Business users

Business users are people who are assigned to one or more user groups based on their responsibilities and authorization levels (role).

If a user is added to a user group in the User Management screen, all the permissions assigned to that group in the permissions scheme will be assigned to the user automatically. In addition to the permissions directly associated with the user group, the user will also be assigned all the (indirect) permissions for the groups to which the user group belongs.

**Please note:** Users should be assigned to a user group that corresponds to their role in the business process as set out in the permissions concept. The process owner in the relevant company is responsible for selecting the user group.

A user can be a member of multiple user groups, including user groups from more than one solution.

---

#### **Please note:**

When a doculife tenant is deployed, no business users (users) other than the **Administrator** user will be set up. Do not change the technical groups to which the administrator is assigned by default, as doing so may mean that the permissions required for administrative tasks may not be available in certain circumstances.

---

Among the various settings for a user account, there is the option of defining a user or user group with management permissions for the account. If a user or user group is given management permissions for a user account, only the **Administrator** user and the user / user group members with the aforementioned management permissions will be able to add the user account to groups.

**Important:** Special administrator rights are required in order to be able to manage users. Please refer to the **Administration rights** section as well.

### Technical user

Technical users provide system functions that are available on all the solutions for a tenant.

---

#### **Please note:**

When a doculife tenant is deployed, the system will set up all technical users automatically.

---

## 7.4 Groups

doculife distinguishes between:

- User groups (roles)
- Groups used to provide access permissions
- Technical groups



## User groups

Users are assigned to a user group based on their responsibilities and authorization levels (role). When a user is assigned to a user group, the user receives the group's permissions (data access and editing permissions) for working in the DMS. This means that each user group is used to group together all the users who need the same data access and editing permissions for files, file types, registers, and documents belonging to a specific confidentiality level.

The naming syntax for user groups is as follows:

- Solution assignment information or solution-specific code
- Information on the access permissions' scope or a role name
- Code Role, R, or User for "user group"

---

**Please note:**

To find out which user groups are available, please refer to the description for your solution.

---

There is the option of defining a user or user group with management permissions for each user group. If a user or user group is given management permissions for a user group, only the **Administrator** user and the user / user group members with the aforementioned management permissions will be able to add users to the group.

## Groups used to provide access permissions

Groups used to provide access permissions are also referred to as "permission groups."

The naming syntax for permission groups is as follows:

- Solution assignment information or solution-specific code
- Information on the access permissions' scope and/or a solution-specific extension
- Code G for "group"

---

**Please note:**

To find out which permission groups are available, please refer to the description for your solution.

---

There is the option of defining a user or user group with management permissions for each permission group. If a user or user group is given management permissions for a permission group, only the Administrator user and the user / user group members with the aforementioned management permissions will be able to add users or groups to the group.

## Technical groups

Technical groups provide essential permissions for internal system processes and the groups associated with them.

## 8 Managing users

### 8.1 Requirement

In order for you to be able to manage a tenant's users, your account must be associated with the corresponding tenant.

---

**Please note:**

Only administrators are allowed to manage users. The administrator creating and managing users is responsible for documenting their creation and management.

---

### 8.2 Adding users

Follow the steps below to add a new user:

1. In Desktop, open the Users management screen by clicking on **Settings, System Configuration, User Management**.
2. Select the **Users** radio button and then click on **Add...**



- You will be able to enter the new user's information in the dialog box that appears.

**New user**

**Assign new user**  
Create a new user

User Type: Full User & Mobile

Login: Mustermann

Name: Max Mustermann

Description (e.g. Email address):  
mustermann@mustermann.com

Managed by: [Select user or group](#)

Password: P2vg#%26VG

Repetition: P2vg#%26VG

Strong password

Show password characters

[Guidelines of secure passwords](#)

Send login data to user

OK Cancel

- Select a user type.

**Important:** When selecting the user type, keep the licenses available to you in mind.

- Enter the following information for the new user:

**Login:** The user's login name

**Important:** Spaces and special characters (ä ö ü \* ? : < > \ /) are not permitted in the login name. Technical user names cannot be used as a login name. If signature-based authorization is used, the label used for the owner when the signature was issued must be used as the login name.

**Name:** The user's display name in doculife

**Description:** Optional

**Managed by:** optional (if necessary, select the corresponding management information for the user. Please refer to the "Assigning management information" section)

**Password:** The user's password (not used if a signature is used for authorization)

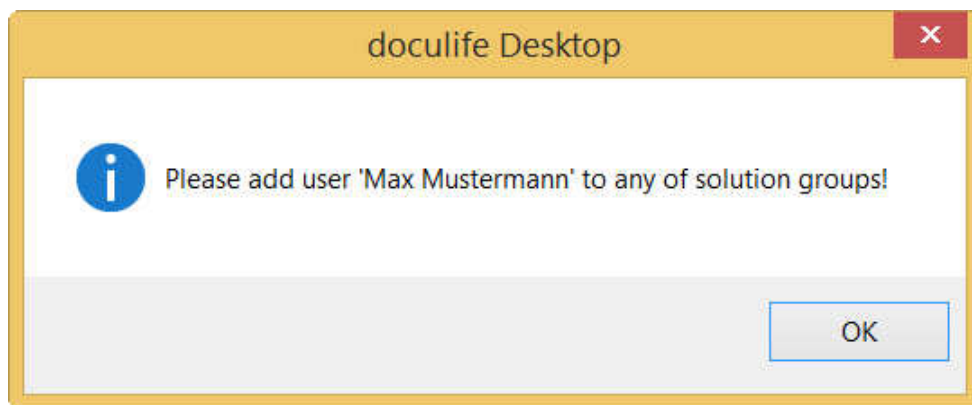
purposes)

**Repetition:** Enter the user's password again (not used if a signature is used for authorization purposes)

**Please note:** Make sure that the password follows the guidelines for strong passwords.

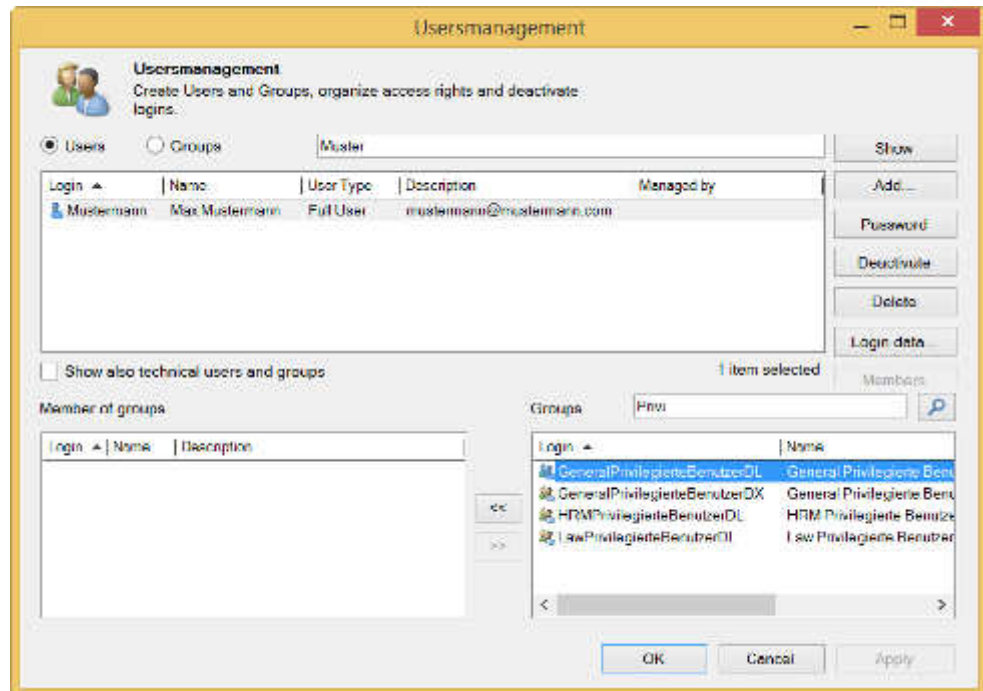
6. When you are done, click on **OK**.
  - If the **Show password characters** check box is enabled, the password's characters will be shown in order to make it easier to ensure that the passwords match.
  - If the **Send login data to user** check box is enabled, the login information will be created after this dialog box is closed so that it can be sent.
7. Send the login information or save it so that you can send it later on.

The login information can be printed out, saved in PDF format, or sent by e-mail. Once you are done, close the window with the login information. If you choose to send the information by e-mail, an activation file will be generated for the user account at the same time and will be provided so that you can send it. Please note that you can send the activation file, login information, and password separately.
8. To assign data access and editing permissions to the user, assign the user to one or more user groups.



Simply click on **OK** in the prompt that appears to this effect.

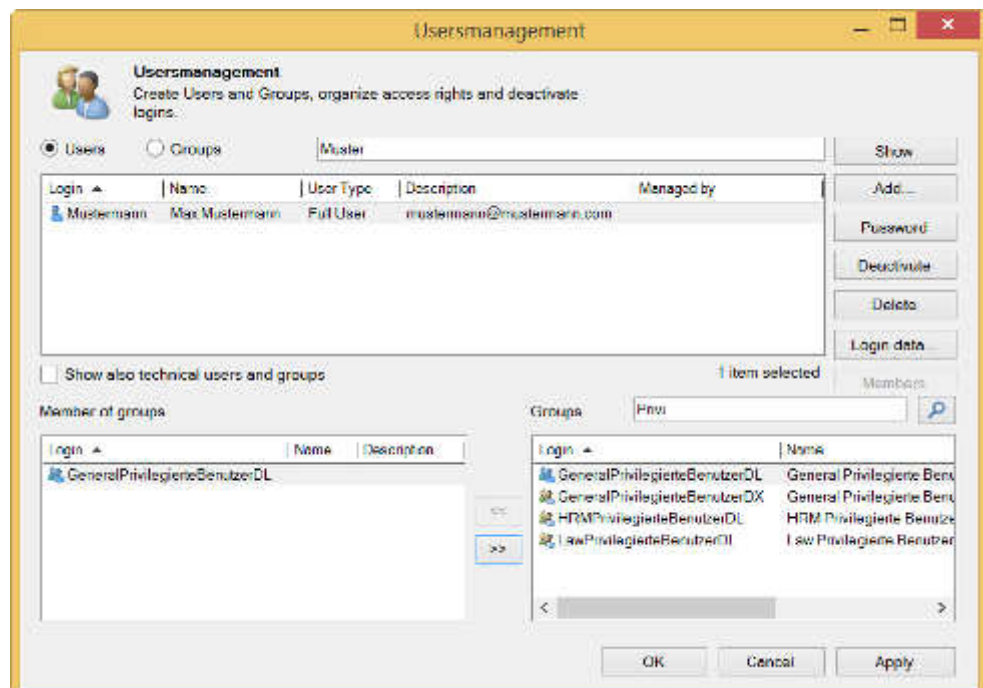
9. Select the user and enter the name of the group to which you want to add the user into the lower search box. It is not necessary to enter the whole name, i.e., entering part of it will be enough. When you do this, all groups with a name containing the text you entered will be shown.



In the **Groups** pane on the bottom right, select the relevant user group(s). Then click on the left arrow icon to add the group(s) to the **Member of groups** pane.

**Please note:** When assigning a user to a user group, make sure to keep the permissions scheme in mind. To find out which user groups are available and what their permissions are, please refer to the description for your solution.

- Click on **Apply** to confirm the changes you have made and close the **User Management** and **Settings** screens by clicking on **OK**.



### 8.3 User types

Whenever you create a user, you will have to assign him or her to a user type. The table below shows all available user types.

User type	Description
<b>Full user</b>	User who accesses the program using Desktop
<b>Full user &amp; mobile</b>	User who accesses the program using Desktop and the mobile client
<b>Web user</b>	User who only accesses the program using WebClient
<b>Web user &amp; mobile</b>	User who accesses the program using WebClient and the mobile client
<b>Web user (read-only)</b>	User who accesses the program using WebClient, but with read permissions only
<b>Web user (read-only) &amp; mobile</b>	User who accesses the program using WebClient and the mobile client, but with read permissions only
<b>Infrequent user</b>	User who accesses doculife only occasionally
<b>Infrequent user &amp; mobile</b>	User who uses the mobile client to access doculife only occasionally
<b>Infrequent user (read-only)</b>	User who accesses doculife only occasionally and with read permissions only
<b>Infrequent user (read-only) &amp; mobile</b>	User who uses the mobile client to access doculife only occasionally and with read permissions only
<b>Self-service user</b>	User who is only allowed to use the self-service mode
<b>Self-service user</b>	User who is also allowed to use the self-service mode on the mobile client

**Important:** When selecting a user type, keep the licenses available to you in mind.

### 8.4 Guidelines for strong passwords

Passwords must meet the following criteria:

- A password must not be blank. It must have at least eight characters.
- The password must be made up of at least three different character groups (lower-case letters, uppercase letters, numbers, symbol characters).
- Especially strong passwords will include characters from all four groups.
- The password must not be one of the last seven passwords used.

### 8.5 Assigning management information

Among the various settings for a user account, there is the option of defining a user or user group with management permissions for the account. If a user or user group is given management permissions for a user account, only the **Administrator** user and the user / user group members with the aforementioned management permissions will be able to add the user account to groups.

To add this management information to a user account, follow the steps below:

1. If:

- You are creating a new user, click on **Select user or group**.

**New user**

**Assign new user**  
Create a new user

User Type: Full User & Mobile

Login: Mustermann

Name: Max Mustermann

Description (e.g. Email address):  
mustermann@mustermann.com

Managed by: [Select user or group](#)

Password: P2vg#%26VG

Repetition: P2vg#%26VG

Strong password

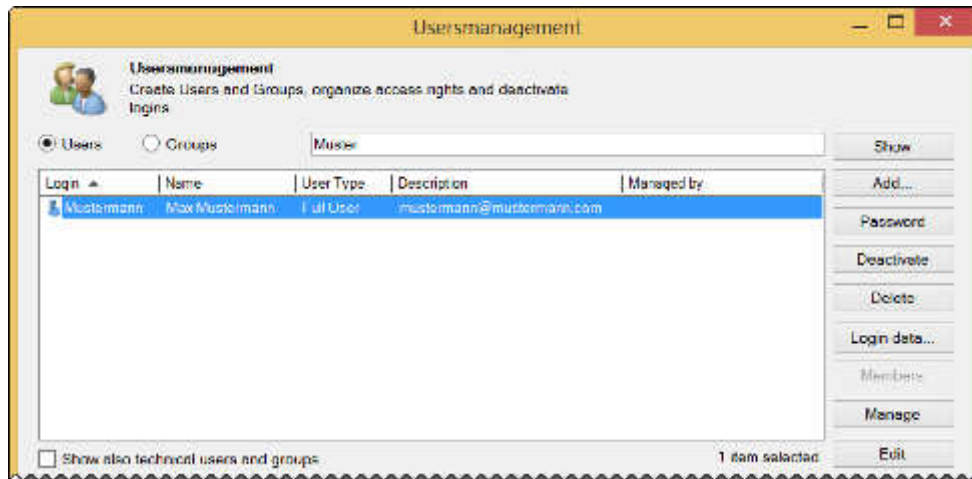
Show password characters

[Guidelines of secure passwords](#)

Send login data to user

OK Cancel

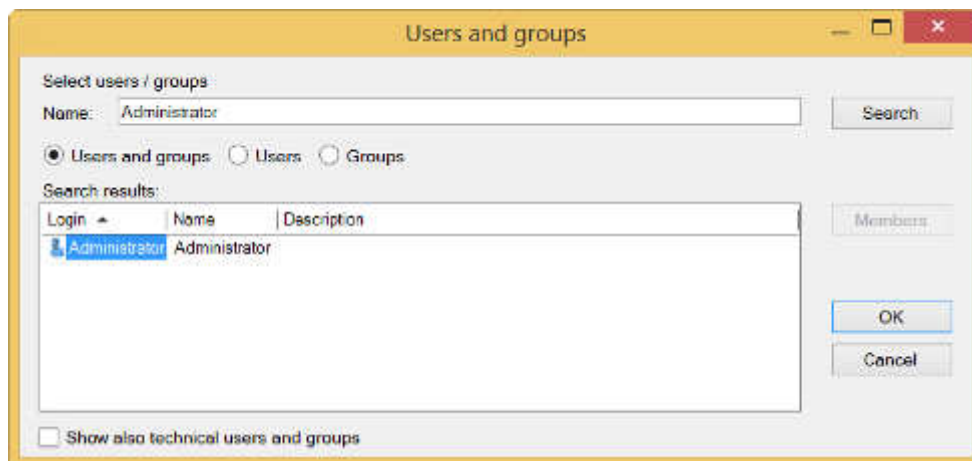
- You are adding management information to an existing user account, select the account and click on **Management**.



2. In the window that appears, enter the name of the user or user group that will manage the user.
3. Click on **Search**.

The user / user group will be shown.

4. Select the user / user group and confirm your selection by clicking on **OK**.



5. Continue with the user creation process or click on **Apply** to confirm the changes you have made and close the **Usersmanagement** window by clicking on **OK**.

## 8.6 Managing users

### 8.6.1 Resetting passwords

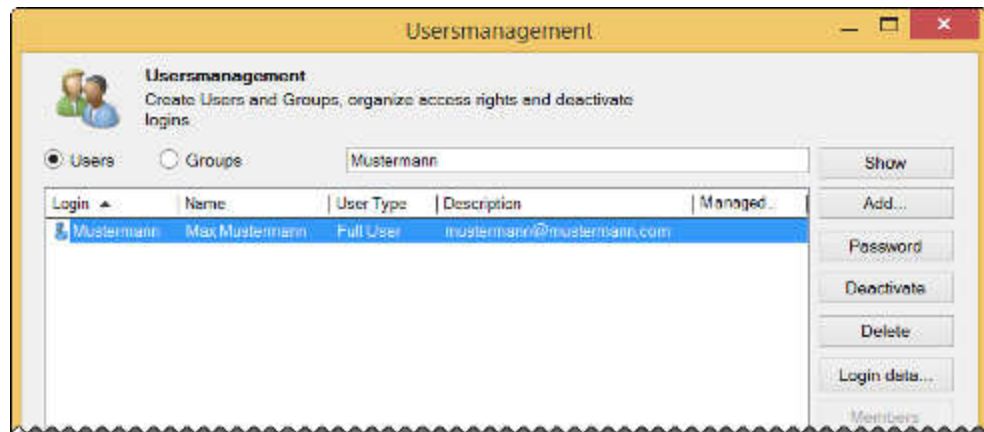
If a user forgets their password, you can use this function to provide the user with a new temporary password. To do so, follow the steps below:

1. Open the **Usersmanagement** screen by clicking on **Settings, System Configuration, User Management**.
2. Select the **Users** radio button. Enter the user's name into the search box and click on **Show**.

The user you are looking for will be shown.



3. Select the user by clicking on them. Click on **Password** or **Login data...**



4. In the password dialog box that appears, enter the new password and then click on **OK**.



If you opened the dialog box by clicking on **Login data**, the login data will be generated in such a way that it will be ready to be sent out.

5. In the prompt that appears, click on **OK**.

---

**Please note:**

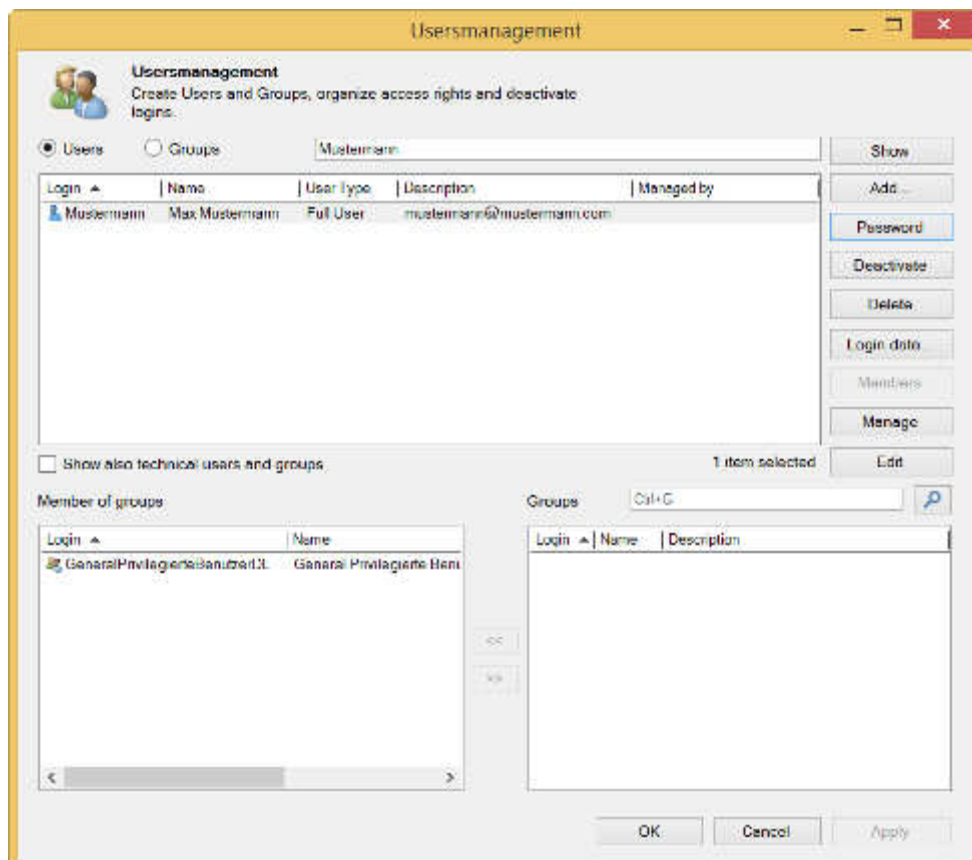
When entering a new password, the password must not be one of the last seven passwords used. Notify the user of the fact that their password has been changed and to provide them with the new password, making sure to observe your company's password rules.

---

## 8.6.2 Changing the groups for a user

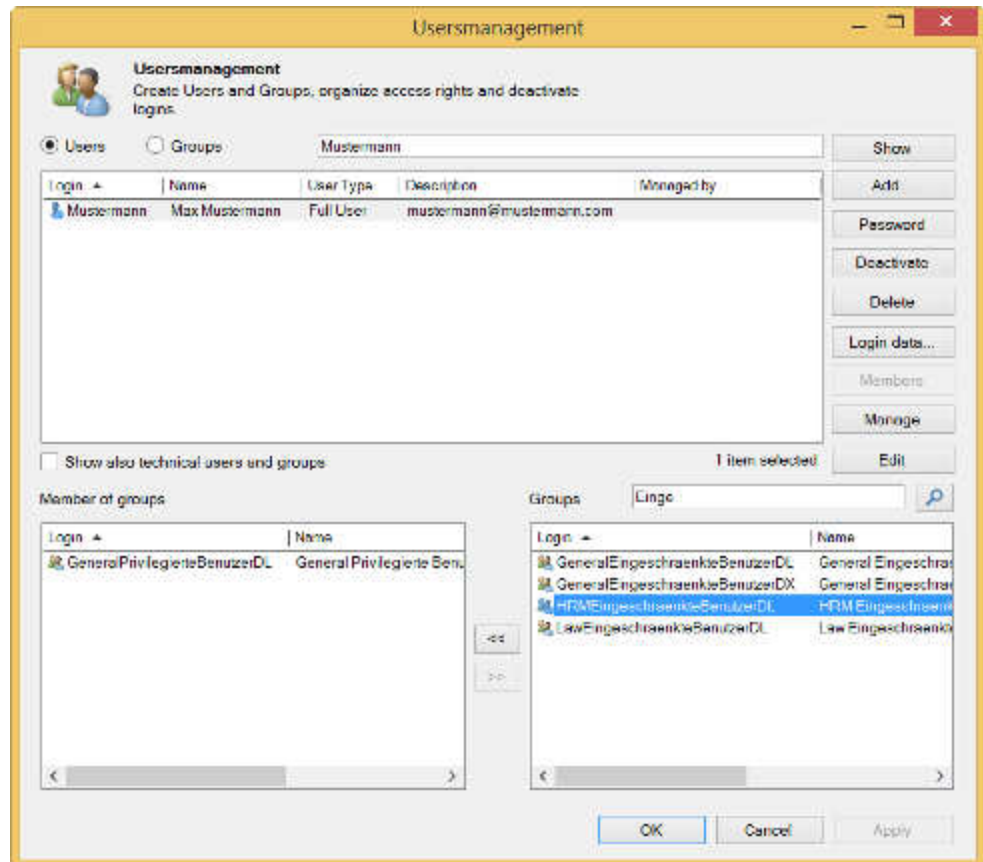
To change the groups for a user, follow the steps below:

1. Open the Usersmanagement screen by clicking on **Settings, System Configuration, User Management**.
2. Select the **Users** radio button. Enter the user's name into the search box and click on **Show**.  
The user you are looking for will be shown.
3. Select the user by clicking on them.  
The Member of groups pane below will show the groups to which the user belongs.



4. Enter the name of the group to which you want to add the user into the lower search box. It is not necessary to enter the whole name, i.e., entering part of it will be enough. When you do this, all groups with a name containing the text you entered will be shown.

In the **Groups** pane on the bottom right, select the relevant user group(s). Then click on the left arrow icon to add the group(s) to the **Member of groups** pane or remove the groups you do not want from the pane by clicking on the right arrow icon.



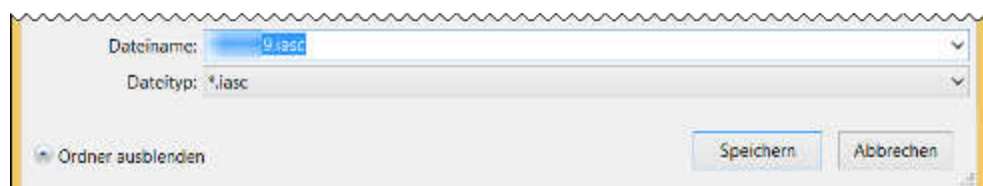
5. Click on **Apply** to confirm the changes you have made and close the **Usersmanagement** window by clicking on **OK**.

### 8.6.3 Sharing scanning activation files

In order to be able to use the direct scanning integration feature in Desktop, the scanning integration feature must first be activated. If the scanning integration feature was not automatically activated while the user account was activated, it will be necessary to activate it separately. To do this, the corresponding user will have to import a scanning key after clicking on **Settings, Profiles, Load Scanning login data**.

These scanning keys can be generated by clicking on **Settings, System Configuration, Share scanning activation**.

1. Click on **Settings, System Configuration, Share scanning activation**.
2. Save the generated \*.iasc activation file.



3. Close the **Settings** window by clicking on **OK**.
4. Send the file to the user so that they can import it.

**Please note:**

If the **Share scanning activation** function is disabled (after you change computers, for example), you can re-enable it by loading the activation key used to activate the tenant.

### 8.6.4 Providing an additional user account for a user

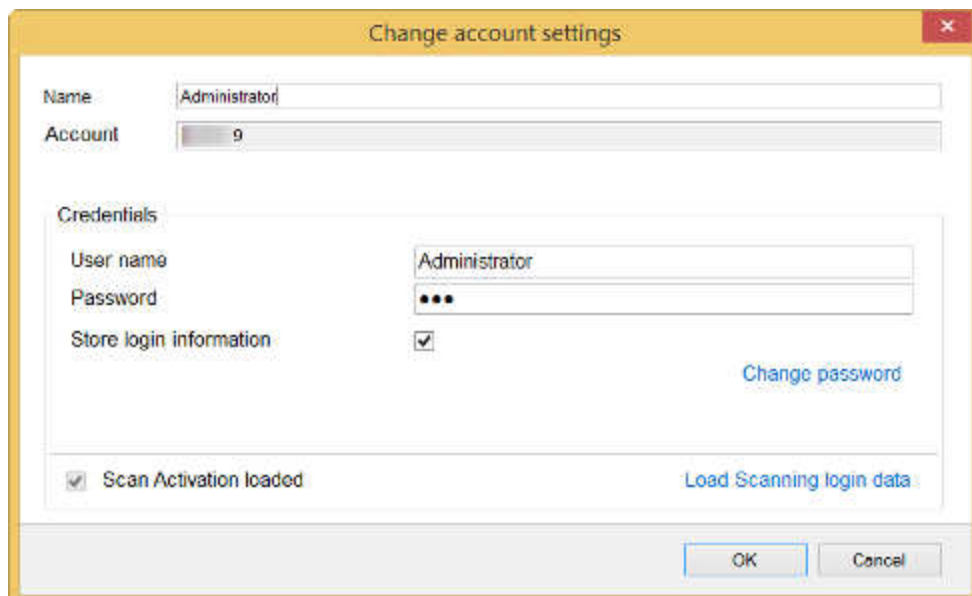
If, for example, you work with doculife both as an administrator and as part of your normal work, it is recommended to use an additional user account for non-administrative tasks.

All you have to do in order to perform the tasks corresponding to the administrator role and to the “normal user” role is to set up an additional user account in the existing setup.

1. **Administrators only**

Give the existing account a name that clearly indicates that it is an administrator account. To do this, go to **Settings, Profiles**, and select the existing account.

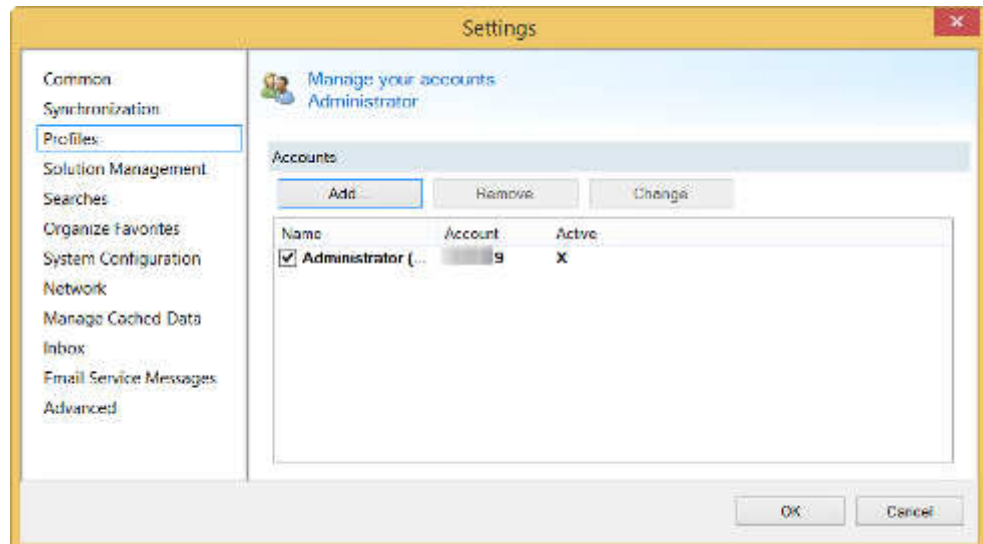
2. Click on **Change** and append the word “administrator” to the account name and then save the change by clicking on **OK**.



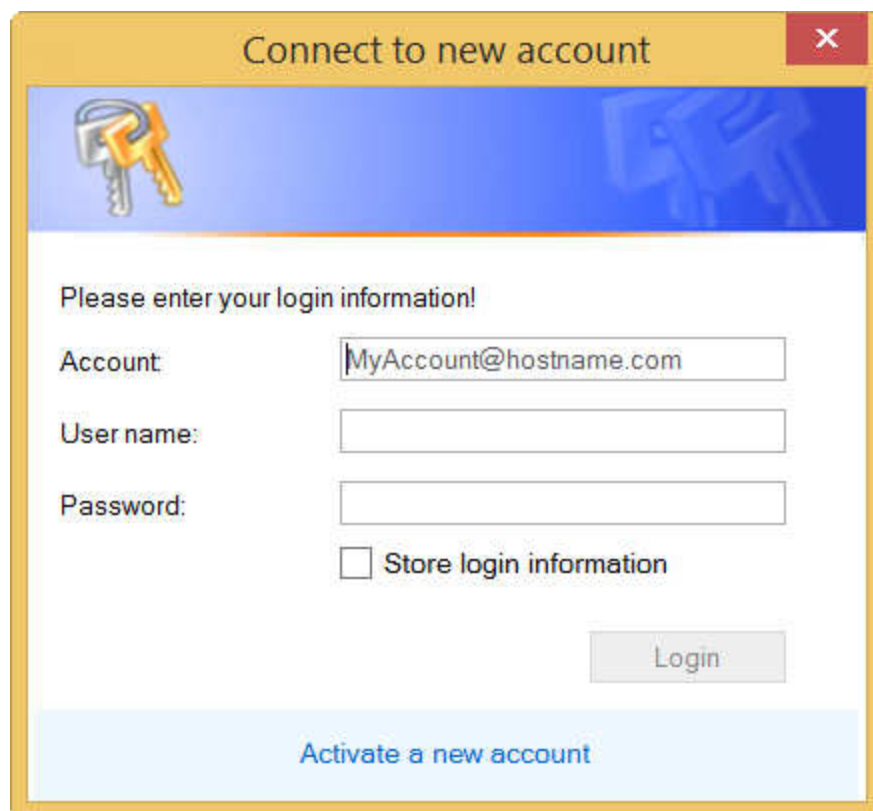
The screenshot shows a dialog box titled "Change account settings". It has a close button in the top right corner. The dialog contains the following elements:

- Name:** A text input field containing "Administrator".
- Account:** A dropdown menu showing "9".
- Credentials:**
  - User name:** A text input field containing "Administrator".
  - Password:** A text input field with masked characters (dots).
  - Store login information:** A checkbox that is checked.
  - Change password:** A blue button.
- Scan Activation loaded:** A checkbox that is checked.
- Load Scanning login data:** A blue button.
- OK** and **Cancel** buttons at the bottom right.

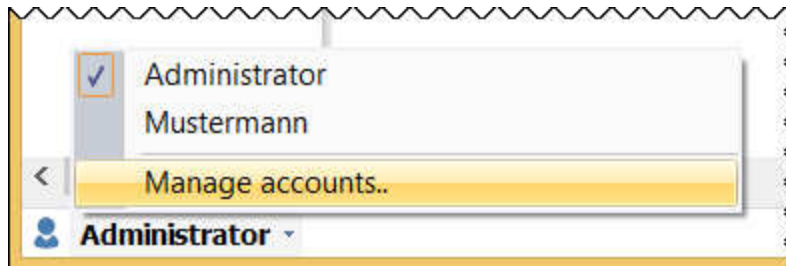
3. Go to the User Management screen and create a new user. Then assign the user to the relevant user group(s) based on the user's functional role within the business.
4. In Desktop, go to **Settings, Profiles** and click on **Add...**



5. In the dialog box that appears, enter your login information and click on **Login** or click on **Activate a new account** and activate the user account with the corresponding activation file.



6. Close the **Settings** window by clicking on **OK**.
7. You will now be able to select the additional user account in the lower left pane in Desktop.



### 8.6.5 Editing user information

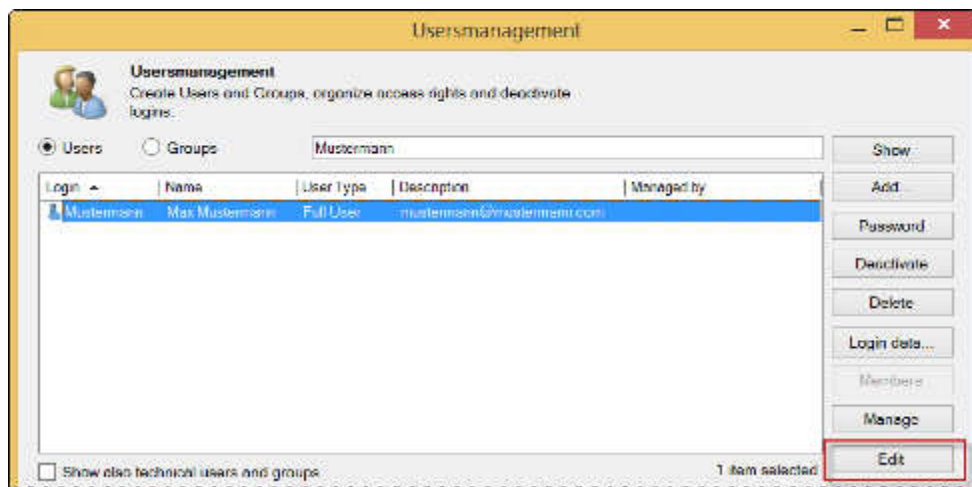
The user information entered when creating a user can be edited at any time.

The following can be changed:

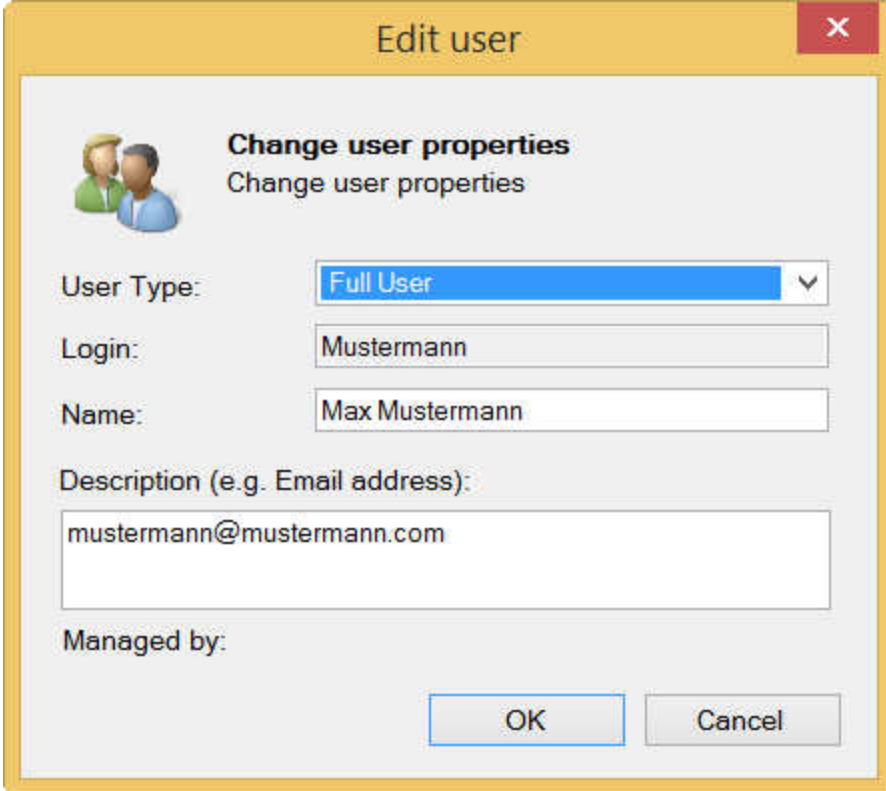
- The type of user
- Name
- Description

To change the user information for an account, follow the steps below:

1. Open the Usersmanagement screen by clicking on **Settings, System Configuration, Usersmanagement**. Enter the user's name into the search box and click on **Show**. The user you are looking for will be shown.
2. Select the user by clicking on them and click on **Edit**.



3. You will be able to make the changes you want in the next window.



**Edit user**

**Change user properties**  
Change user properties

User Type: Full User

Login: Mustermann

Name: Max Mustermann

Description (e.g. Email address):  
mustermann@mustermann.com

Managed by:

OK Cancel

4. To confirm your changes, click on **OK**.

## 8.7 Closing a user account

### 8.7.1 When to close an account

Close a user account:

- When a user leaves the organization in an organized fashion: After the user's tasks and documents are transferred to their successor.
- Immediately as soon as you become aware of a user leaving due to unforeseeable circumstances.
- Immediately whenever there is an "imminent danger situation" related to the user.

### 8.7.2 Deactivating a user account

---

**Please note:**

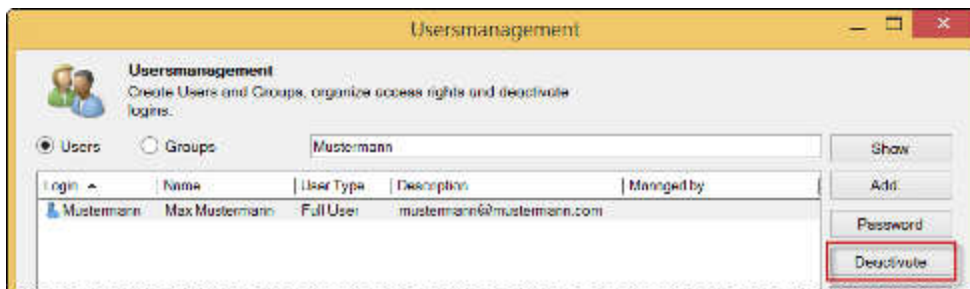
Before deactivating a user account, check to make sure that every single step required in order to prepare for deactivating the account has been completed. Before deactivating the user account, take control of the account and monitor the whole process. Remove the user from all user groups.

---

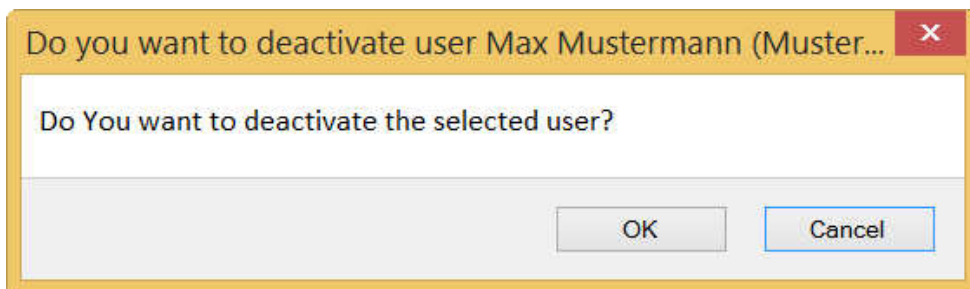
Follow the steps below to deactivate a user account:

1. In Desktop, open the Users management screen by clicking on **Settings, System Configuration, User Management**.
2. Call up the user you want and take control of the user account by resetting its password.
3. Log in with the new login information.

4. Check the contents in the user's personal **inbox**. Forward these contents to the user's replacement if necessary or move them to their final storage location. Once you are done, empty the recycle bin completely.
5. Check whether the user still has documents checked out. If possible, check these documents back in from the user's workstation or cancel the checkout.
6. Check whether there are any tasks that have not been completed or that are currently pending under **Tasks**. Find out who will be responsible for completing these tasks.
7. Check whether there is any data stored in the **My Documents** folder. If there are any documents in it, find out what should be done with them. Once you are done, empty the folder completely.
8. Check the user's **recycle bin**. Find out whether any documents in it are still needed or whether they should be permanently deleted. Restore any documents that are still needed and delete all others. Once you are done, empty the recycle bin completely.
9. Remove all links from the user's **My Workplace** and **library**.
10. Go to **Settings, Inbox, Settings** and disable the option allowing the inbox to receive e-mails. Disable the option allowing the inbox to be used for external forwarding. Empty the list of whitelisted forwarding and sender addresses.
11. Go to **Settings, Inbox, Settings** and delete all the group inboxes to which the user had access.
12. Close the user account, log in as an administrator, and open the **Usersmanagement** screen.
13. Call up the user's account and remove it from all groups.
14. Click on **Deactivate**.



15. In the prompt that appears, click on **OK**.

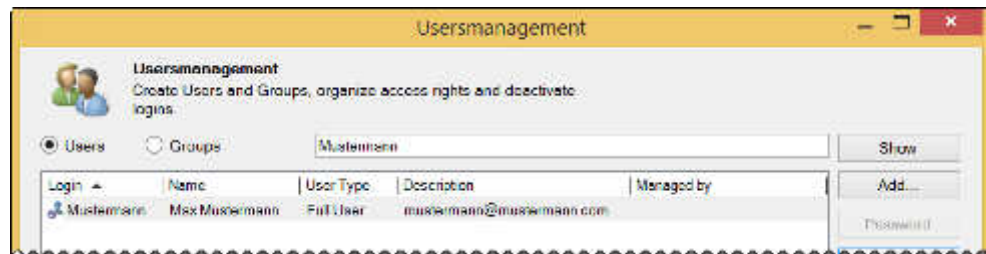


16. Click on **Apply** to confirm the changes you have made and close the **User Management** and **Settings** screens by clicking on **OK**.

The user will be shown as being deactivated the next time the Usersmanagement



screen is opened.



---

**Please note:**

Once you deactivate the user account, it will no longer be possible to access their personal workplace.

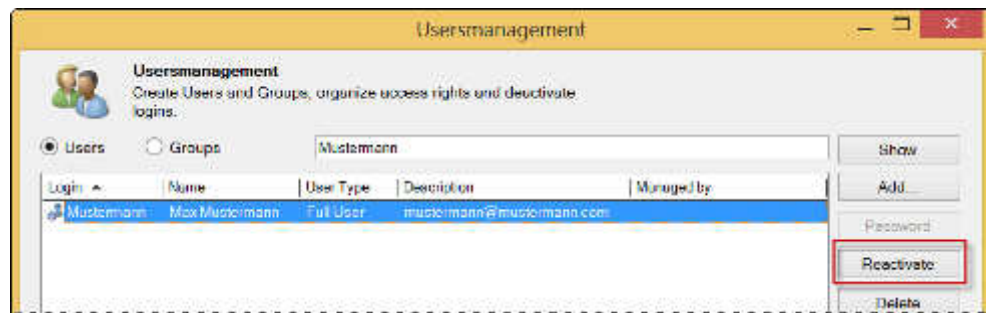
---

### 8.7.3 Reactivating a user account

Deactivated user accounts can be reactivated.

To reactivate a user account, follow the steps below:

1. In Desktop, open the Users management screen by clicking on **Settings, System Configuration, User Management**.
2. Call up the deactivated user account you want and click on **Reactivate**.



3. In the prompt that appears, click on **OK**.



4. Select the user and enter the name of the group to which you want to add the user into the lower search box. It is not necessary to enter the whole name, i.e., entering part of it will be enough. When you do this, all groups with a name containing the text you entered will be shown.

In the **Groups** pane on the bottom right, select the user group(s) to which you want to

add the user. Then click on the left arrow icon to add the group(s) to the **Member of groups** pane.

5. Click on **Apply** to confirm the changes you have made.
6. Edit the user data for the account if necessary. Click on **Edit** to open the corresponding dialog box. Click on **OK** to confirm the changes you make.

The screenshot shows a dialog box titled "Edit user" with a yellow border. Inside, there is a header "Change user properties" with a sub-header "Change user properties" and a user icon. The form contains the following fields:

- User Type: Full User (dropdown menu)
- Login: Mustermann (text box)
- Name: Max Mustermann (text box)
- Description (e.g. Email address): mustermann@mustermann.com (text box)
- Managed by: (empty text box)

At the bottom of the dialog are "OK" and "Cancel" buttons.

7. If necessary, select new management information for the user. To do so, click on **Manage**. Enter the name of the user or user group that will manage the user into the search box. Click on **Search**.

The user / user group will be shown.

8. Select the user / user group and confirm your selection by clicking on **OK**.
9. Assign the user a new password. Click on **Password** or **Login data...** In the password dialog box that appears, enter the new password and then click on **OK**.

Notify the user of the fact that their login data has been changed and provide them with the new data.

10. Close the Usersmanagement window by clicking on **OK**.

#### 8.7.4 Deleting a user account

---

**Please note:**

Deleting user accounts is not recommended for doculife installations in which BusinessOwnerG has not been implemented. In general, it is recommended to only delete user accounts if they have never been used before.

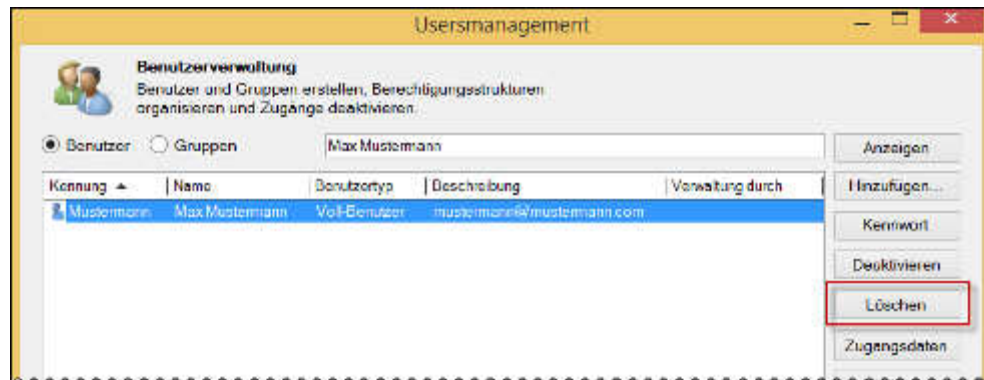
---

To delete a user, follow the steps below:

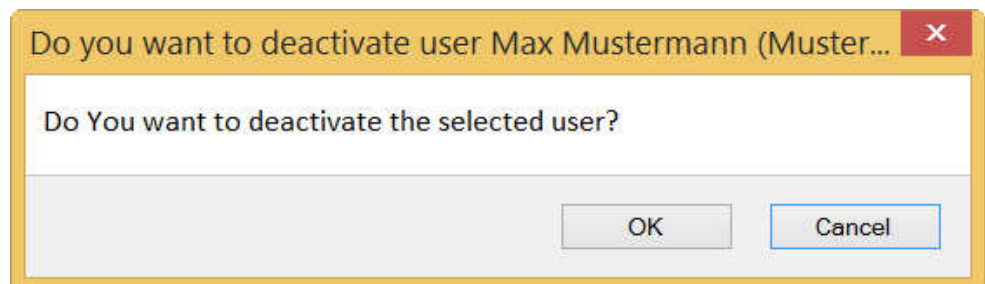
1. In Desktop, open the Users management screen by clicking on **Settings, System Configuration, User Management**.
2. Call up the user account you want.

**Important:** Make sure that the user account has not been used yet. If the user account has already been used, carry out all the steps required in order to deactivate the user (please refer to the “Deactivating a user account” section) before deleting the account.

3. Select the user account and click on **Delete**.



4. In the prompt that appears, click on **OK**.



5. Close the **User Management** window by clicking on **OK**.

## 8.8 Overview of technical users

Technical users provide system functions that are available on all the solutions for a tenant.

The following technical users are used in doculife:

Name	Description
Audit	Audit/event service - Logs application events triggered by users and technical users in the audit
EmailService	E-mail service – Runs the e-mail-based functions available in the DMS
Export	Export service - Provides contents for full-text searches
Import	Import service – Imports the files and metadata delivered by the IMA system components and through third-party system web services into the DMS
MDI	MDI service – Processes information delivered through web services

Name	Description
	(Master Data Integration interface)
OSAdmin	Technical administration user
SystemService	System service for archiving processes
TempAccess	Automatically enables temporary access when the latter is granted; not used in doculife as of this writing
Template	Technical user for managing templates
u1 - un	Upload user 1 to n

---

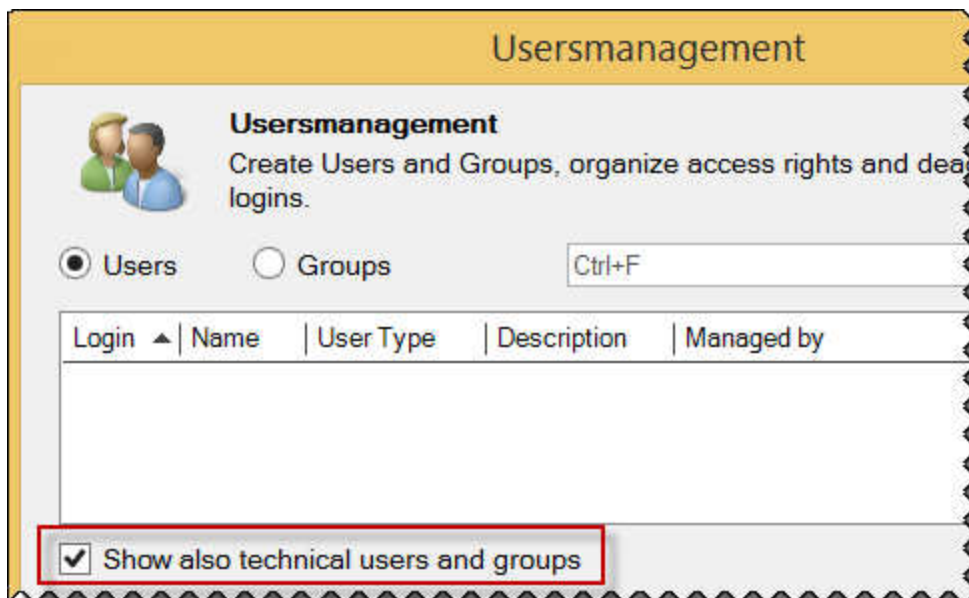
**Please note:**

When a doculife tenant is deployed, the system will set up all technical users automatically. Technical users cannot be managed using the Usersmanagement screen.

---

## 8.9 Displaying technical users

- ▶ To have the system display technical users as well, enable the **Show also technical users and groups** option in the User Management screen.



**Important:** If you enable this option, business users and technical users will both be shown together.

## 9 Managing groups

### 9.1 Overview

In order to make the task of managing groups easier, users need to be added to one or more user groups based on their role.

User groups receive permissions by belonging to one or more groups used to provide access permissions (permission groups).

Permission groups get their access permissions from the technical groups to which they belong.

When a user is assigned to a user group or a group is assigned to another group, all the permissions defined in the permissions scheme will be assigned to the user / to the first user group automatically.

When a user or user group is assigned to a user group, the user / the first group will not only become a member of the user group to which it has been assigned (direct membership), but will also inherit any memberships corresponding to that user group. In other words, the user / user group will also become a member of the groups to which the parent user group belongs (indirect membership).

### 9.2 Adding a user group

Additional user groups can be added to solutions.

---

**Please note:**

Make sure to add new user groups only in accordance with the permissions system corresponding to the solution being used. If you have any questions, please contact your solution vendor or doculife Support.

---

Follow the steps below to add a user group to a solution:

1. Open the **User Management** screen by clicking on **Settings, System Configuration, User Management**.
2. Select the **Groups** radio button and click on **Add...**
3. In the dialog box that appears, enter the information required in order to create the group.

**New group**

**Assign new group**  
Create a new group

Name:

Complete Name:

Description (e.g. Email address):

Managed by: [Select user or group](#)

OK Cancel

**Name:** Name of the group

**Please note:** Spaces and special characters (ä ö ü \* ? : < > \ /) are not permitted in group names. Add code letter **R** (for user groups) at the end of the name.

**Complete Name:** The group's display name in doculife

**Description:** Optional

**Managed by:** Management information - optional

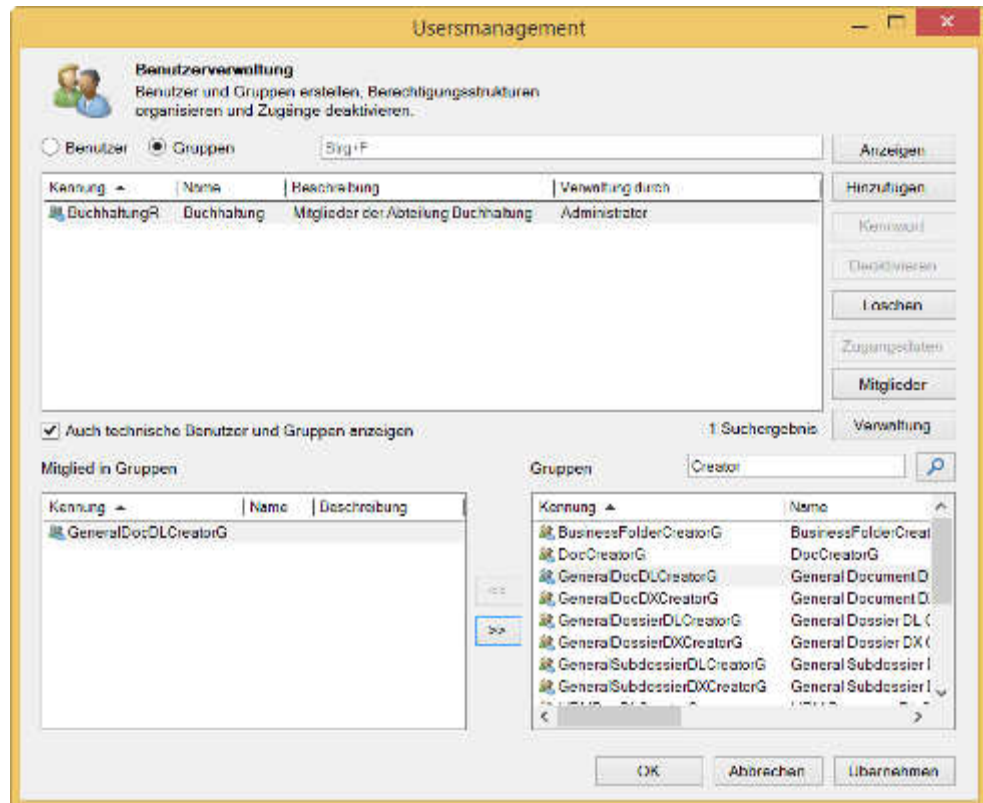
4. Close the dialog box by clicking **OK**.
5. To assign data access and editing permissions to the group, select the group and then enter the name of the group to which you want to add the original group into the lower search box. It is not necessary to enter the whole name, i.e., entering part of it will be enough.

When you do this, all groups with a name containing the text you entered will be shown.

To have the program also show technical groups, enable the **Show also technical users and groups** option.

**Please note:** If you enable this option, business groups and technical groups will both be shown together.

In the **Groups** pane on the bottom right, select the user group(s) to which you want to add the group. Then click on the left arrow icon to add the group(s) to the **Member of groups** pane. Click on **Apply** to confirm your selection.



6. Close the **User Management** window by clicking on **OK**.

---

**Please note:**

If you do not add the newly added group to another group, the group will not have any data access or editing permissions.

Once you are done, open the Usersmanagement screen and assign users to the group you created based on their functional role within the business. To do this, call up each user account individually and add it to the group (Member of groups).

---

### 9.3 Showing the members of a group

Follow the steps below to find out which users currently belong to a group:

1. Open the **User Management** screen by clicking on **Settings, System Configuration, User Management**.
2. Select the **Groups** radio button, enter the name of the group you want into the search box, and click on **Show**.
3. Then select the group and click on **Members**.

Group members will be shown with their name, login, and a “Membership through” comment that explains how they are a member of the group.



4. Click on **Close** to exit the list.

### 9.4 Displaying group memberships

When a user is assigned to a user group or a group is assigned to another group, all the permissions defined in the permissions scheme will be assigned to the user / to the first user group automatically.

When a user or user group is assigned to a user group, the user / the first group will not only become a member of the user group to which it has been assigned (direct membership), but will also inherit any memberships corresponding to that user group. In other words, the user / user group will also become a member of the groups to which the parent user group belongs (indirect membership).

---

**Please note:**

The user groups to which other user groups are assigned by default (selection when a custom solution is activated or loaded) should not be altered, as the solution(s) installed for a tenant may stop working properly under certain circumstances.

---

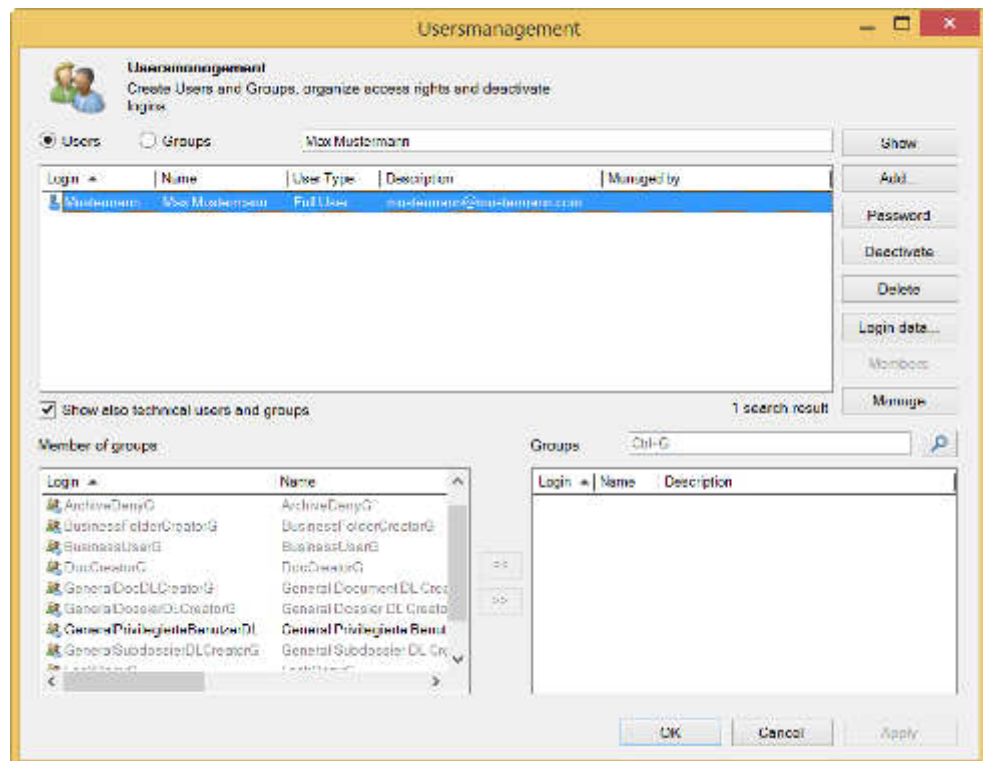
To display the groups to which a user or group is assigned, follow the steps below:

1. Open the **User Management** screen by clicking on **Settings, System Configuration, User Management**.



- To view the groups to which a user belongs, select the **Users** radio button. Enter the user's name into the search box and click on **Show**. To view the technical groups to which the user belongs, enable the **Show also technical users and groups** option.
- Select the user in order to look at the groups to which they belong.

The corresponding memberships will be shown.



Direct memberships will be shown using black text, while indirect memberships will be shown using gray text.

- To view the groups to which a group belongs, select the **Groups** radio button. Enter the group's name into the search box and click on **Show**. To view the technical groups to which the user belongs, enable the **Show also technical users and groups** option.
- Select the group in order to look at the groups to which it belongs. The corresponding memberships will be shown.  
Direct memberships will be shown using black text, while indirect memberships will be shown using gray text.

Making individual changes to the implemented permissions concept and the permissions scheme is possible at any time. For more detailed information, please contact your solution vendor or doculife Support.

## 9.5 Groups used to provide access permissions

Groups used to provide access permissions are also referred to as "permission groups."

They provide user groups with solution-specific permissions for creating and editing objects based on the permission system's permissions scheme.

In solutions with a single-level security context, user groups are directly assigned to technical groups with creation permissions. The following technical groups with creation permissions will be available for each solution:

- Group with permission to create files (DossierCreatorG)
- Group with permission to create registers (SubdossierCreatorG)
- Group with permission to create documents (DocCreatorG)

To have the system display these groups, enable the **Show also technical users and groups** option in the Usersmanagement screen.

In solutions with a multi-level security context, user groups are assigned to solution-specific permission groups. These permission groups provide permissions indirectly through their membership in technical groups with creation permissions.

Additional permission groups can be added to solutions.

---

**Please note:**

Make sure to add permission groups only in accordance with the permissions scheme corresponding to the permissions system of the solution being used. If you have any questions, please contact your solution vendor or doculife Support.

---

## 9.6 Technical groups

Technical groups provide essential permissions for internal system processes and the groups associated with them.

- **Technical groups with creation permissions that apply to all solutions:**  
Used to provide all user groups with the permissions assigned according to the permissions scheme, e.g., for creating items belonging to classes used commonly (file, e-mail, multimedia).
- **Technical groups with function permissions that apply to all solutions:**  
These bundle internal system permissions for the use of DMS functionalities based on a defined group hierarchy (group is a member of group) and provides them to the user groups based on the permissions scheme.

### Technical groups with creation permissions that apply to all solutions

Name	Description
BusinessFolderCreatorG	Group that provides permissions for creating files, registers
DocCreatorG	Group that provides permissions for creating basic-class documents (computer files, e-mail, multimedia)

### Technical groups with function permissions that apply to all solutions

Name	Description
ACLAdminG	Group that groups together the permissions for managing permissions
AdminAccessG	Group used to provide administration rights for accessing all data
AdminOperationG	Group used to provide permissions for select administrative functions (audit, reports, choice lists)

Name	Description
ArchiveDenyG	Technical DMS archive group
ArchiveG	Group used to provide permissions for archiving items
ArchiveOwnerG	Technical DMS archive group
BusinessUserG	Group that provides user groups with the required permissions for using DMS applications
ChoicelistAdminG	Group used to provide permissions for managing choice lists
DisableSystemG	Technical DMS system administration group
LDAPAdminG	Group used to provide permissions for managing users and groups
LDAPBusinessAdminG	Group used to provide limited permissions for managing users and groups
LockDenyG	Reserved, not used in doculife as of this writing
LockOwnerG	Reserved, not used in doculife as of this writing
ManagementG	Group used to provide permissions for editing solution configurations
OSAdminG	Technical DMS administrator group
OSUserG	Technical DMS user group
PrintG	Group used to provide permissions for using an optional print service; not used in doculife as of this writing
ReactivationG	Group used to provide permissions for reactivating archived items
ReportG	Group used to provide permissions for the server-side reporting functionalities
SettingAdminG	Technical DMS system administration group
TechnicalUserG	Group used to provide permissions for the functionalities for technical users
TempAccessG	Group used to provide permissions for granting temporary access; not used in doculife as of this writing
TemplatesAdminG	Group used to provide permissions for managing templates
ViewAuditG	Group used to provide permissions for viewing audits

To have the system display technical groups as well, enable the **Show also technical users and groups** option in the User Management screen.

---

**Please note:**

The assignment of technical groups to other technical groups should not be altered, as the solution(s) installed for a tenant may stop working properly under certain circumstances.

---

## 9.7 Deleting groups

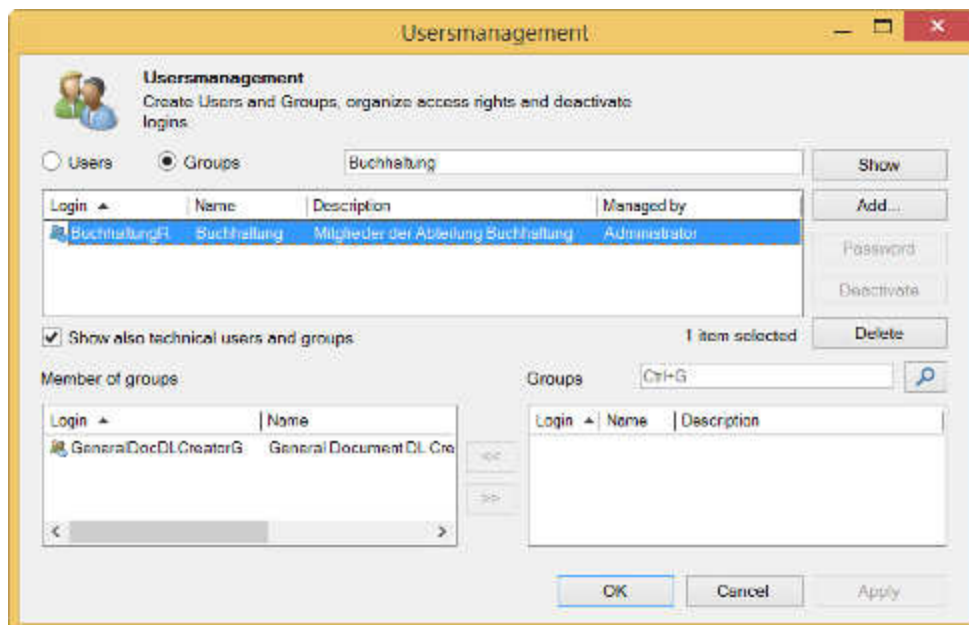
### Please note:

In certain cases, deleting a group may cause the solution(s) installed for a tenant to stop working properly. If you have any questions, please contact your solution vendor or doculife Support. Technical groups cannot be deleted.

**Important:** Before deleting a group, make sure to first remove all users from that group.

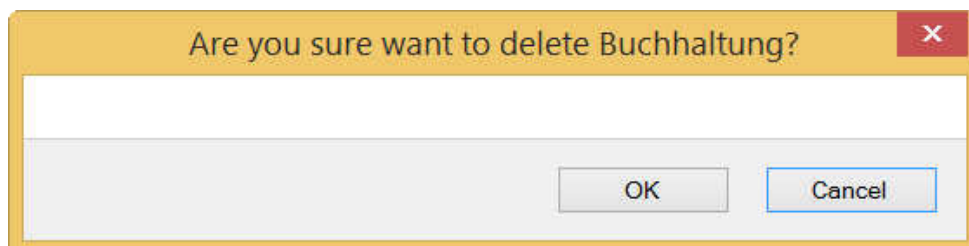
To delete a group, follow the steps below:

1. In Desktop, open the Users management screen by clicking on **Settings, System Configuration, User Management**.
2. Call up the group you want.
3. Select the group and remove it from all groups. Click on **Apply**.



4. Then click on **Delete**.
5. In the prompt that appears, click on **OK**.

The group will be deleted.



## 10 SECplus / SECmezzanine key administration

### 10.1 Overview

---

**Please note:**

The following functions are available for doculife SECplus and SECmezzanine tenants only.

---

When documents are transferred between a client and the doculife cloud service using the transport layer, they are encrypted as well (HTTPS/SSL). Once the documents are on the server, a full text index is generated on the server and the documents are stored in a secure, tamper-proof repository after being encrypted with 256-bit AES. Finally, the corresponding metadata, as well as the full text index itself, is stored in encrypted databases.

Generally speaking, encryption on the server is organized in such a way that the operator does not have any access to document, metadata, and encryption contents.

---

**Please note:**

For more information on how encryption works and its scope, please contact your solution vendor or hosting provider.

---

The user is the one who sets the aforementioned key, as well as the one who manages it and uses it to unlock the tenant. This ensures that:

- Authorized users can prevent any access to the corresponding data by locking the tenant
- Technical staff and IT administrators will **not have any access to the customer's data**, since the tenant is automatically fully locked when technical work is being performed and the data for the tenant cannot be viewed as a result.

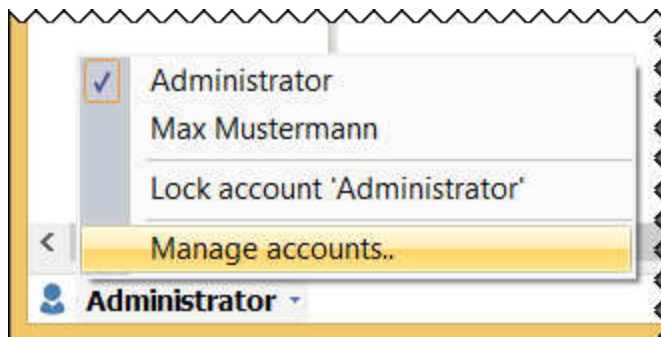
The following applies in terms of how the key is used and managed:

- The administrator sets the key during initialization (first use with the \*.idac activation key)
- The tenant can be locked at any time by any user with the corresponding permissions
- The tenant can be unlocked by any user who has the corresponding key
- The key can be changed by any user who has locking permissions

### 10.2 Locking tenants

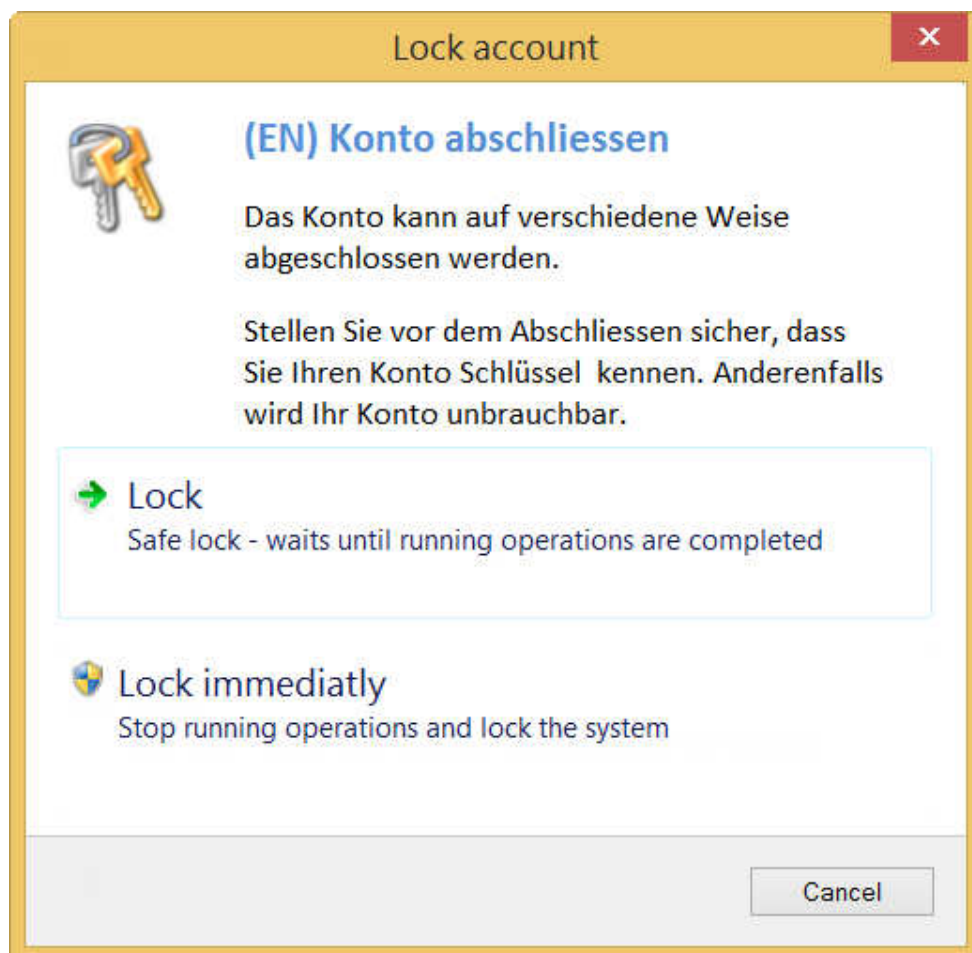
To lock a tenant, follow the steps below:

1. Select the **Lock account** option on the bottom left of the Desktop.



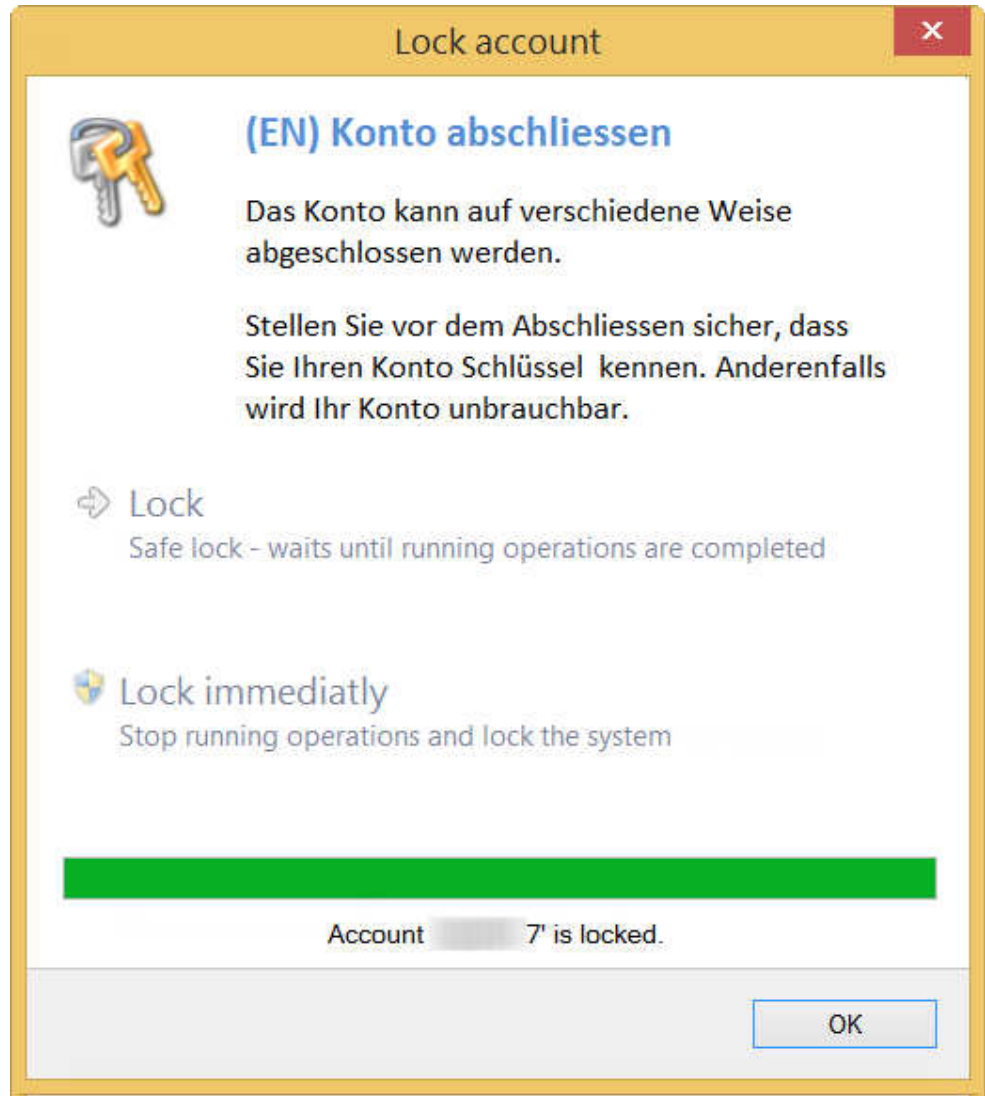
2. Select the type of lock you want.

- **Lock** - The tenant will be locked after any ongoing actions being carried out by users are completed, e.g., ongoing file imports with drag & drop
- **Lock immediately** - The tenant will be locked immediately Any user actions that are still ongoing will be aborted



3. In the prompt that appears, click on **OK**.

The tenant is now locked.



### 10.3 Granting permissions for locking a tenant

To grant permissions for locking a tenant, add the corresponding user to the **AdminOperationG** technical group.

---

**Please note:**

Assigning the user to the **AdminOperationG** group will give them additional permissions. Before adding the user, make sure that their functional role in the business process allows for these permissions to be assigned to them. For more information regarding the permissions associated with belonging to these groups, please refer to the chapter "Granting management permissions".

---

**Important:** The key can be changed by any user who has locking permissions.

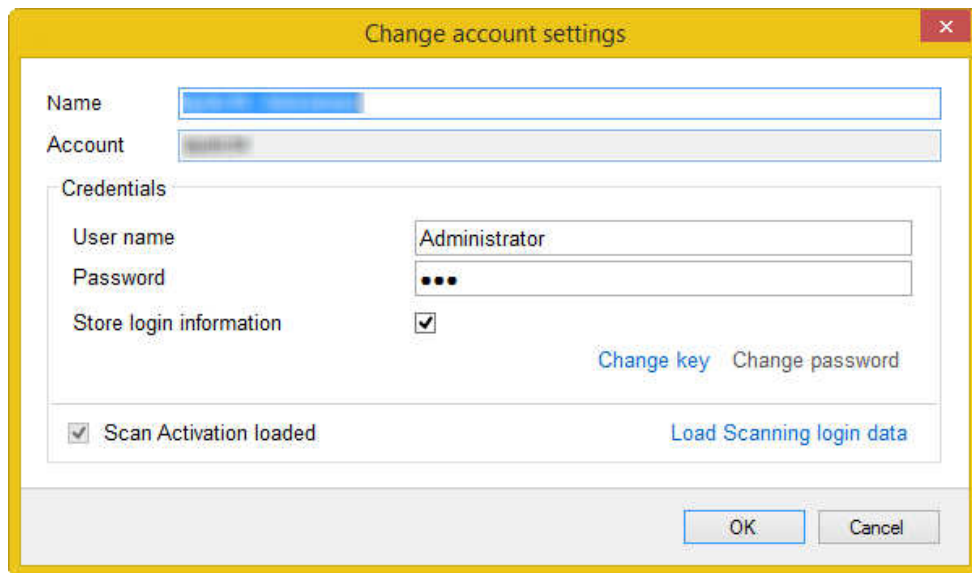
## 10.4 Changing keys

**Please note:**

Make sure that the user making the change safely stores the key afterwards and notifies other key owners. This is especially important, as locked tenants cannot be unlocked without a valid key and keys cannot be reset by administrators.

The key can be changed by any user who has locking permissions.

1. Click on **Settings, Profiles**. Select your user account, and click on **Change**.
2. Click on **Change key**.



The screenshot shows a dialog box titled "Change account settings" with a yellow border and a close button in the top right corner. The dialog contains the following elements:

- Name:** A text input field with a blue selection bar.
- Account:** A text input field with a greyed-out value.
- Credentials:** A section containing:
  - User name:** A text input field with the value "Administrator".
  - Password:** A text input field with masked characters (dots).
  - Store login information:** A checkbox that is checked.
- Buttons:** "Change key" and "Change password" are blue text links.
- Other options:** A checkbox for "Scan Activation loaded" (checked) and a blue text link "Load Scanning login data".
- Bottom buttons:** "OK" and "Cancel" buttons.

3. Change the key. Confirm by clicking on **OK**.



### Change key of your account

**(EN) Änderung Ihres Konto Schlüssels**

Bitte wählen Sie einen Schlüssel, den Sie sich gut merken können und der den angezeigten Richtlinien entspricht. Beachten Sie, dass Ihr Konto unbrauchbar wird, falls Sie diesen Schlüssel vergessen sollten. Im Sinne der Hochsicherheitsanforderungen für Ihre Daten gibt es keine Möglichkeit, den Schlüssel durch den Dienstanbieter zurücksetzen zu lassen.

Wählen Sie hier einen Schlüssel, um Ihr Konto auf- und abzuschliessen:

**Choose here a key to lock/unlock your account:**

Old Key:

New Key:

Repeat key:

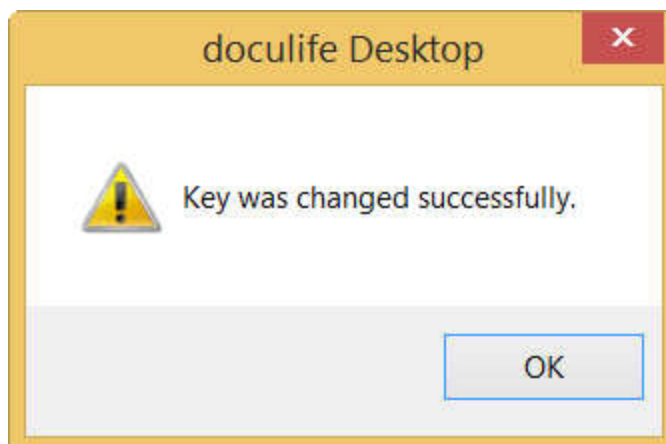
Show key characters

OK Cancel

4. Save or print the key. Confirm the prompt reminding you to safely store the key by enabling the corresponding checkbox, then click on **OK**.



5. Confirm the key change by clicking on **OK**.



**Important:** Once the key is changed, the tenant will be locked and will need to be unlocked by someone with the appropriate permissions.

## 11 Inboxes

### 11.1 Overview

Inboxes are an important tool in the teamwork between users and user groups.

Inboxes can be used to assign incoming documents to a user or user group for review and editing. Moreover, using the **forwarding** DMS function in conjunction with inboxes makes it possible to initiate, carry out, and monitor agile workflows for editing and approving documents. Inboxes are also e-mail inboxes for the corresponding enabled doculife e-mail addresses.

There are two types of inboxes in doculife:

- Personal inboxes
- Group inboxes

Personal and group inboxes are created automatically in doculife when a user or group is created. A personal inbox is automatically activated and enabled the first time the corresponding user logs in. Meanwhile, group inboxes must be activated and enabled by the administrator before they can be used.

### 11.2 Personal inboxes

A personal inbox is automatically activated and enabled the first time the corresponding user logs in. A personal inbox:

- contains documents forwarded to the user for editing
- is the inbox for the user's doculife e-mail address
- can be used as a default scan input folder

The contents in a personal inbox can only be viewed and edited by the corresponding user.

### 11.3 Group inboxes

Every user group has its own group inbox, and the members of a user group can connect to the corresponding group inbox and view and edit its contents. A group inbox:

- Contains documents forwarded to the group for editing
- Is the inbox doculife for the group's e-mail address
- Can be used as a default scan input folder

Group inboxes are created automatically when a group is set up. However, before the group inbox can be used, the administrator needs to activate it.

## 11.4 Managing inboxes

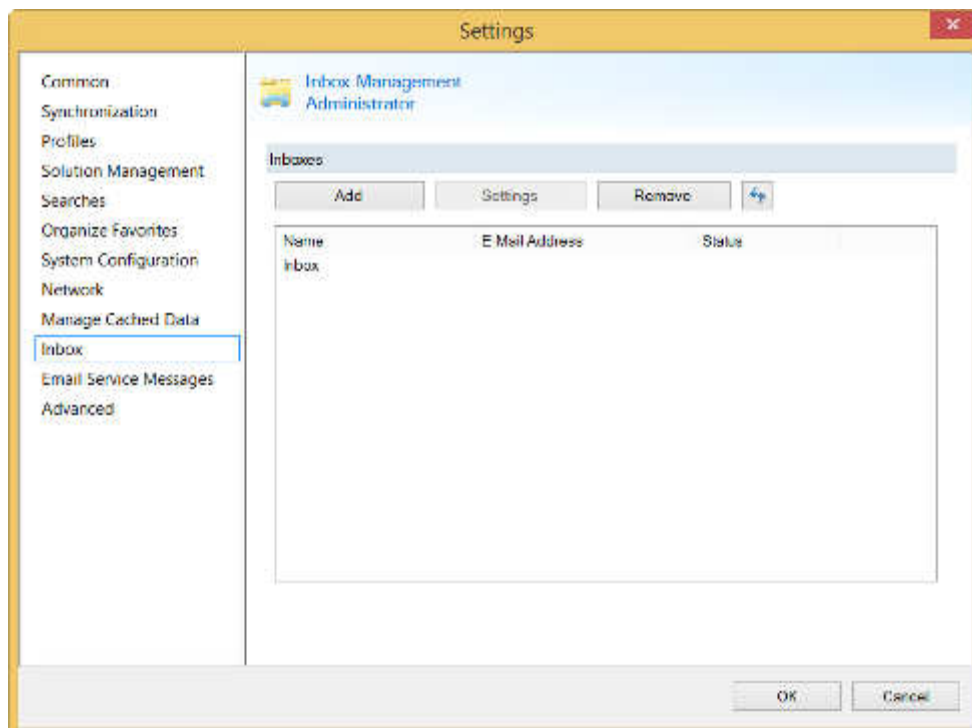
### 11.4.1 Adding inboxes to the inbox overview

Follow the steps below to get an overview of the inboxes that are available and the inboxes that are in use:

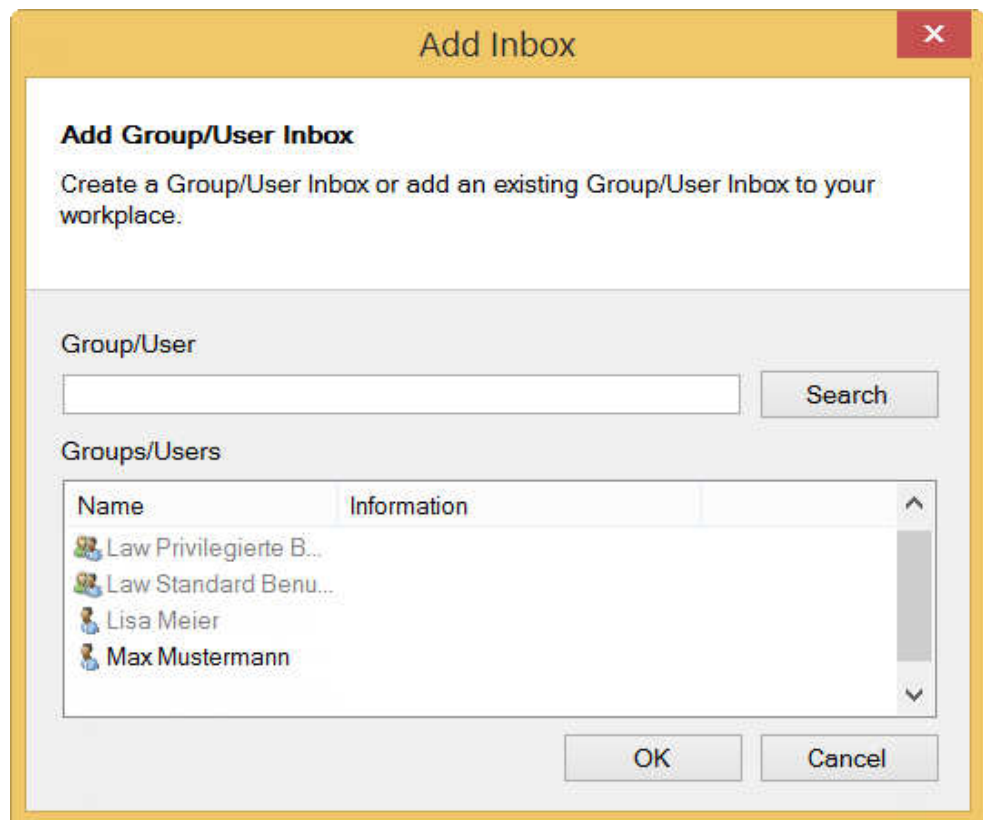
1. Click on the **Settings** menu option and then on **Inbox**.

The following screen will show the inboxes to which you (the administrator) have access. Your personal inbox will be named **Inbox**.


2. Click on **Add**.



3. Enter the name of the user or user group you want into the **Group/User** field and click on **Search**.




The relevant user and user group inboxes will be shown in the bottom pane.

-  group inboxes will be displayed as follows:

**Grey:** Disabled inbox

**Black:** Enabled inbox

-  Personal inboxes will be displayed as follows:

**Grey:** After the user is created, but only until the user logs in for the first time

**Black:** Black font colour afterwards

4. If you select an inbox and close the dialog box by clicking on **OK**, the inbox will be added to your **Inbox Management** overview.

## 11.4.2 Opening and working with a user's inbox

---

### **Please note:**

The functionality for viewing the contents of personal inboxes can only be used by administrators.

---

A user's personal inbox can only be opened and viewed by that user. However, certain circumstances (such as the user being absent for an extended period of time unexpectedly) may make it necessary for an administrator to open or empty a personal inbox in order to make it possible for other users to access the documents in the inbox so that they can work with them.

## Opening personal inboxes

To view the full contents of a user's personal inbox, add the inbox to your **Inbox Management** overview. Open the inbox under **My Workplace**.

Once you are done, remove the inbox from your **Inbox Management** overview. Simply select the inbox and click on **Remove**.

## Working with personal inboxes

Take control of the user account by changing the user password in the Usersmanagement screen. Log in to the DMS with the user account.

### Tip:

To make sure you won't get mixed up with other inboxes to which you have access, use a separate instance of Desktop portable to log in.

Click on **Forward** to make the relevant documents accessible to the people who need to work on them or drag and drop them onto a different file.

Reset the user account's password once you are done. Make sure to notify the user accordingly.

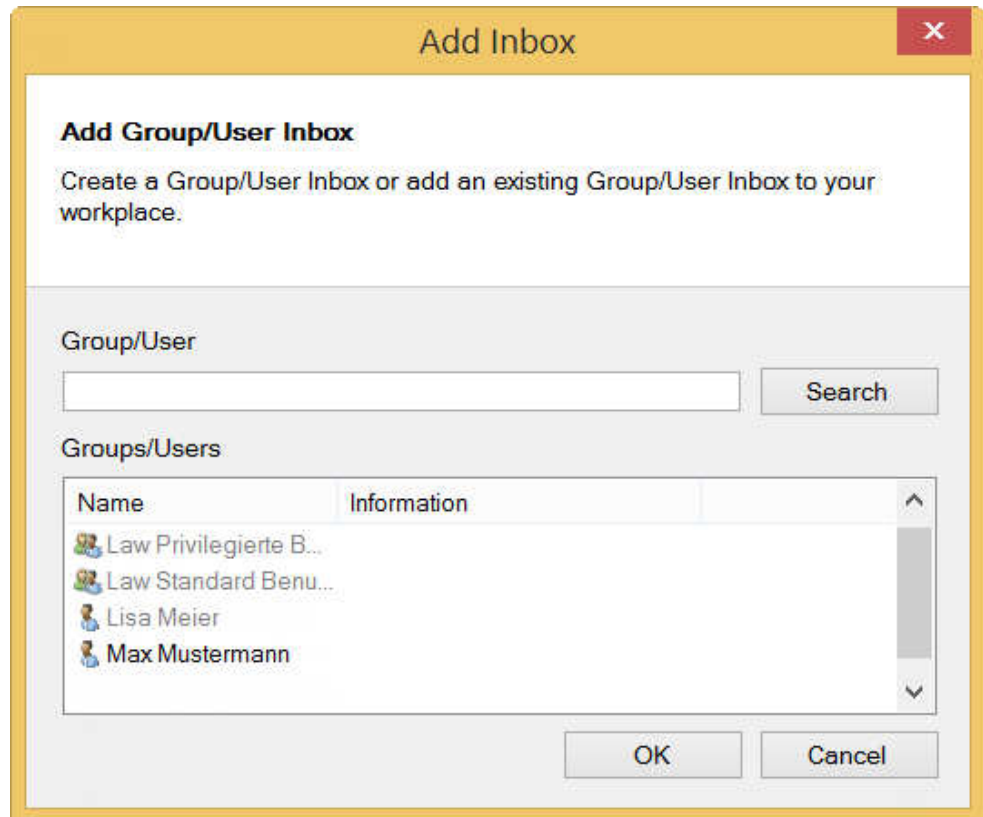
## 11.4.3 Group inbox

### 11.4.3.1 Enabling group inboxes

Follow the steps below to enable a group inbox so that it can be used by the members of a user group:

Open the screen used to manage inboxes by clicking on **Settings, Inbox, Add**.

1. In the **Group/User** field, enter the name of the user group for which you want to enable a group inbox. Then click on **Search**.
2. The inbox that will be enabled will be shown in the pane at the bottom. Then click on **OK**.



The group inbox will be enabled and added to your **Inbox Management** view.

Once the inbox is enabled, all members of the corresponding user group will be able to add the group inbox to their workplace by clicking on **Settings, Inbox, Add**.

3. If you will not be needing the enabled group inbox later on, you can remove it from your **Inbox Management** view. Simply select the inbox and click on **Remove**.

---

**Please note:**

For more information on how to use inboxes, please refer to the user manual for doculife Desktop.

---

#### 11.4.3.2 Opening and working with group inboxes

Group inboxes can only be opened and worked with by members of the corresponding user group.

However, certain circumstances (such as all the members of the user group being absent) may make it necessary for an administrator to open or empty a personal inbox in order to make it possible for other users to access the documents in the inbox so that they can work with them.

##### Opening group inboxes

To view the full contents of a group inbox, add the inbox to your **Inbox Management** overview. Open the inbox under **My Workplace**.

##### Working with group inboxes

Use the Usersmanagement screen to add yourself to the relevant group. Open the group inbox and click on **Forward** to make the relevant documents accessible to the people who

need to work on them or drag and drop them onto a different file.

Once you are done, remove the inbox from your **Inbox Management** overview. Simply select the inbox and click on **Remove**. Restore the permissions for working with the group inbox to the way they were previously by removing yourself from the corresponding group in the Usersmanagement screen.



## 12 Finding documents

Documents stored in a user's **personal inbox** or **My Documents** folder cannot be viewed by other users.

---

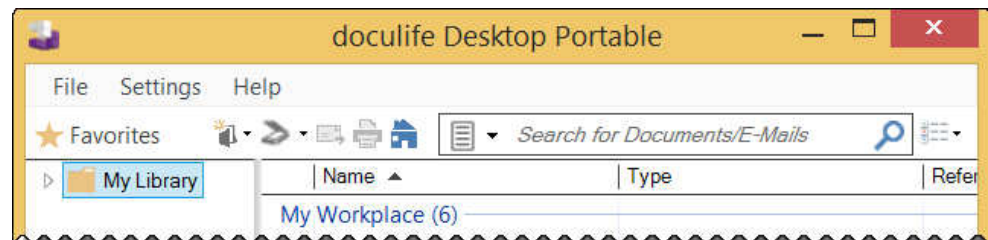
**Please note:**

The functionality for finding documents in personal inboxes and My Documents folders can only be used by administrators.

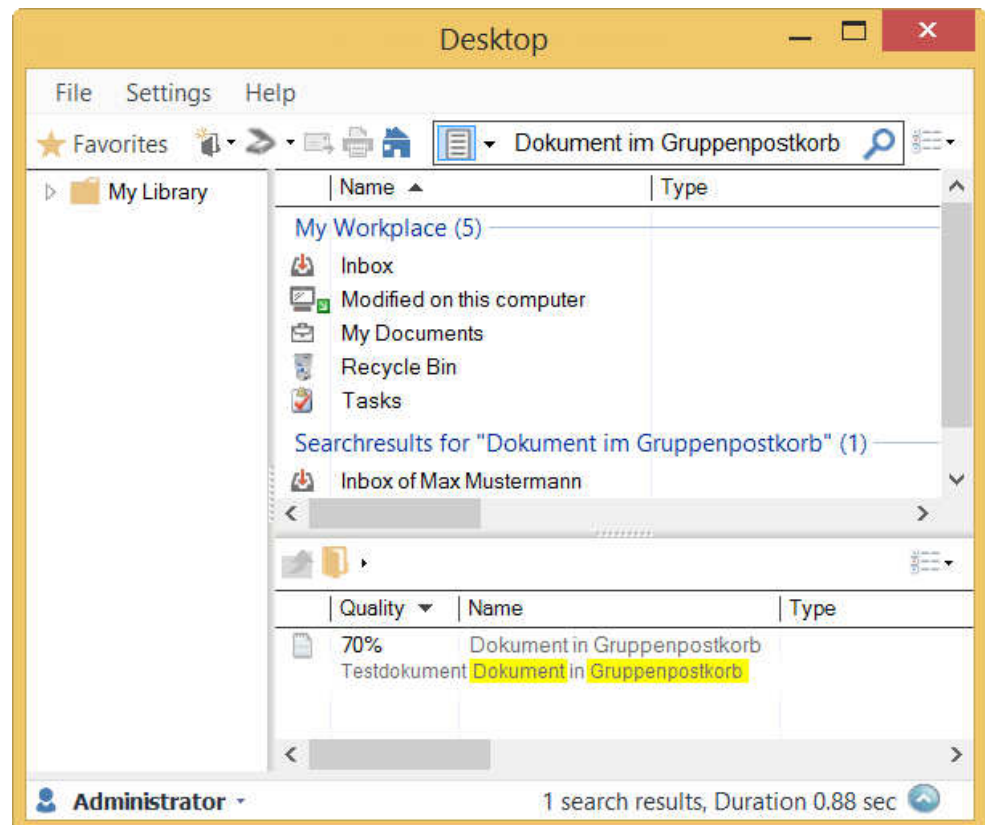
---

If necessary, an administrator can find out which user has a specific document stored in their personal inbox or My Documents folder.

1. To do this, use the **All Documents**, **Data Files** and **E-Mails** search option.



2. Enter the name of the document you are searching for or a relevant term from the document's contents into the search field and run the search.



The results will show the document and the inbox in which the document is found.

## 13 Solution administration

### 13.1 Overview

Solutions can be customized and expanded at any time. You can do the following yourself:

- Customize and expand choice lists
- Create searches and make them available to all users
- Modify templates found in the solution

or

- Send templates found in the solution to your solution vendor so that they can carry out a change request
- Order an update or a custom solution (\*.zip)
- Order a customized feature set from your solution vendor

Customizations carried out by you, as well as change requests, updates, and individual solutions, can be made available to all users by using the **Save/Publish Templates** function.

### 13.2 Saving templates in the filesystem

---

**Please note:**

Advanced administrator rights are required in order to be able to save templates in the filesystem.

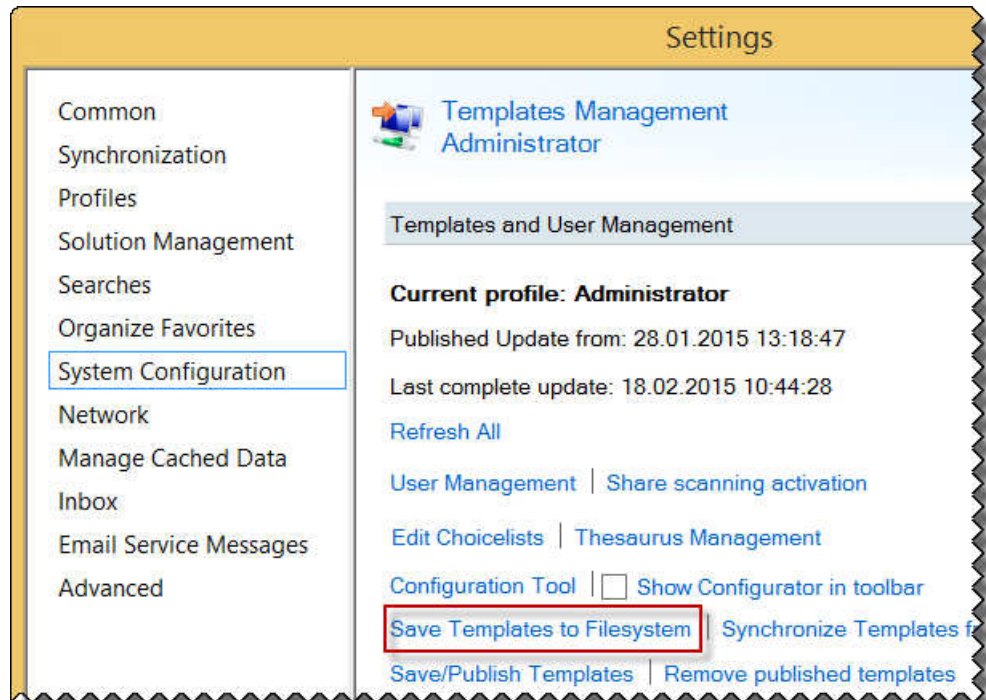
---

Back up your current solution before:

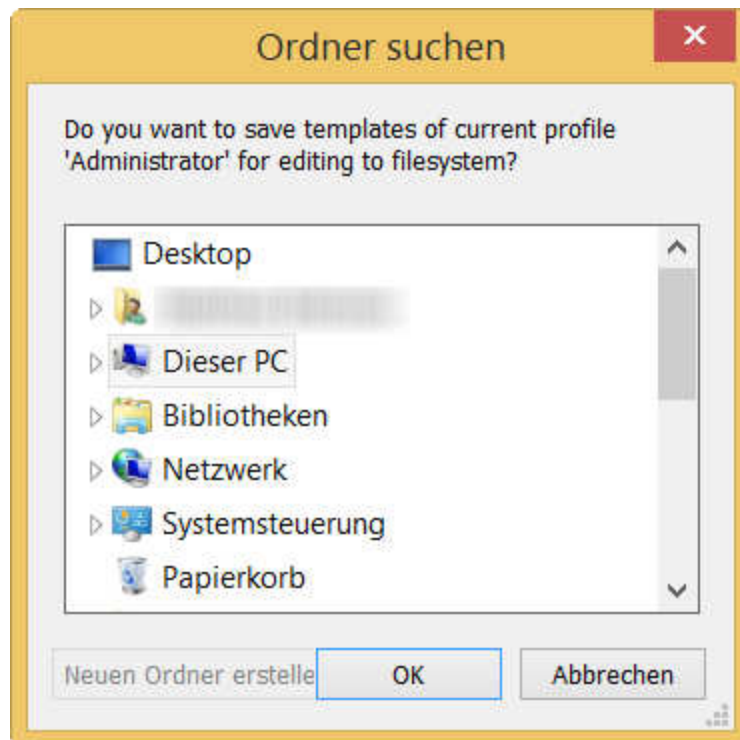
- Editing choice lists
- Making searches available to other users
- Modifying templates found in the solution
- Loading a change request or a custom solution

To back up the solution you are currently using, follow the steps below:

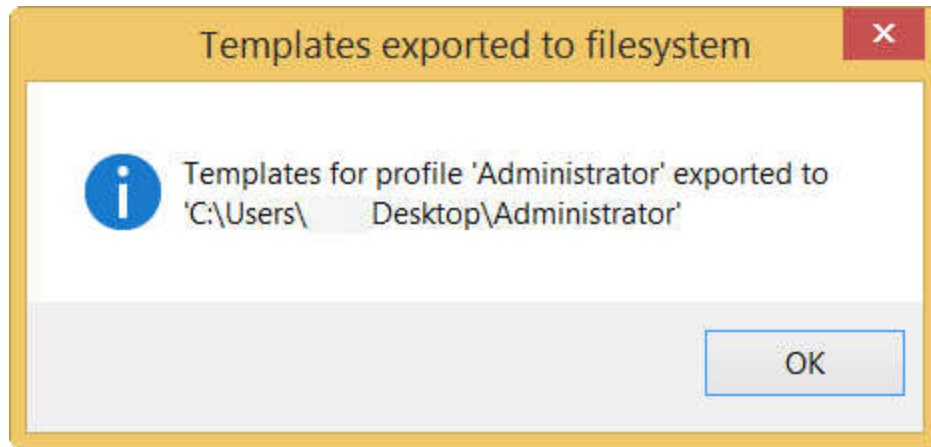
1. Click on **Settings, System Configuration**. Click on **Save Templates to Filesystem**.



2. In the next dialog box, select a storage location and confirm your selection by clicking on **OK**.



3. In the prompt that appears, click on **OK**.



**Important:** Give the download a unique name. Store it safely. Direct changes to templates should not be made using the original templates. Instead, copy the folder with the templates before making changes.

## 13.3 Creating searches

### 13.3.1 Creating searches

doculife Desktop users can create personal search templates for themselves in addition to the default searches available. Administrators can make their own personal search templates available to all users as default searches.

---

**Please note:**

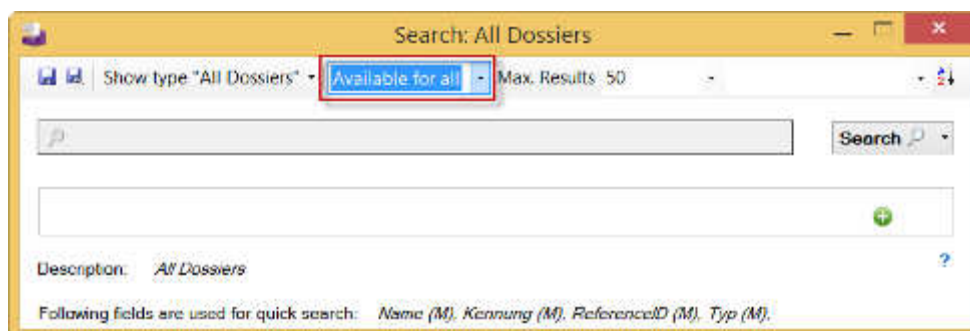
For information on how to create new searches, please refer to the “Working with personal search templates” section found in the user manual for doculife Desktop.

---

### 13.3.2 Making available to all users

To make a search template available to all users, follow the steps below:

1. To create the search template, follow the steps in the “Working with personal search templates” section of the user manual for doculife Desktop.
2. Select the option **Available for all**.



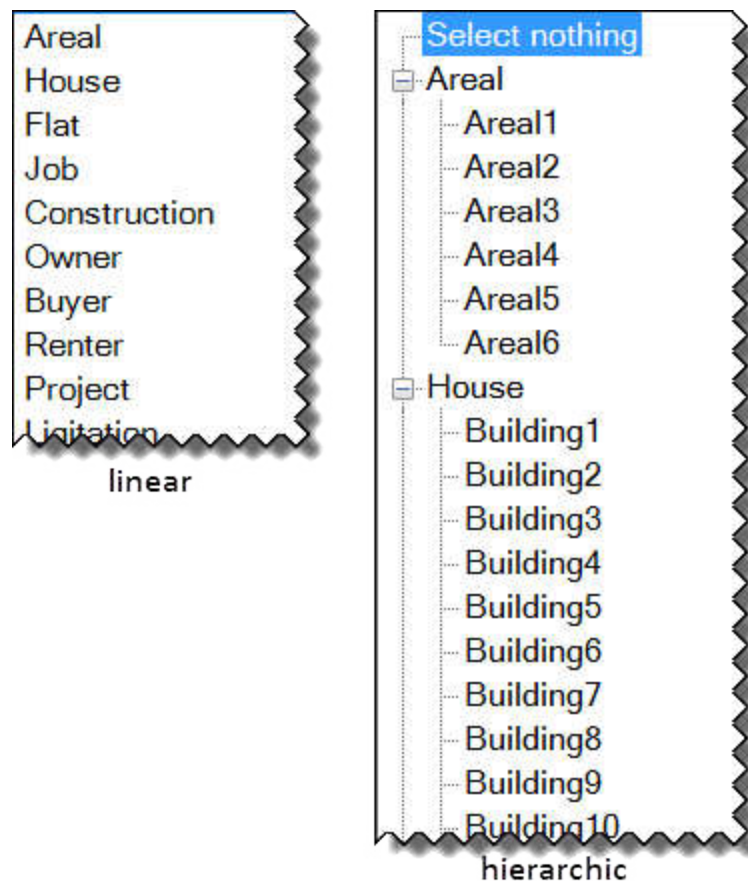
3. Save the search template using the name you want to use in order to make the template available to all users (e.g. file number search).

## 13.4 Choice lists

### 13.4.1 Overview

Choice lists make it possible to provide users with selectable entries for file, register, and document index fields. Values not included in a choice list cannot be entered into the index field associated with the choice list.

Choice lists can either be simple (single-level) choice lists or cascaded (multi-level) choice lists.



**Important:** When working with cascaded choice lists, please note that nodes cannot be selected as index values.

---

**Please note:**

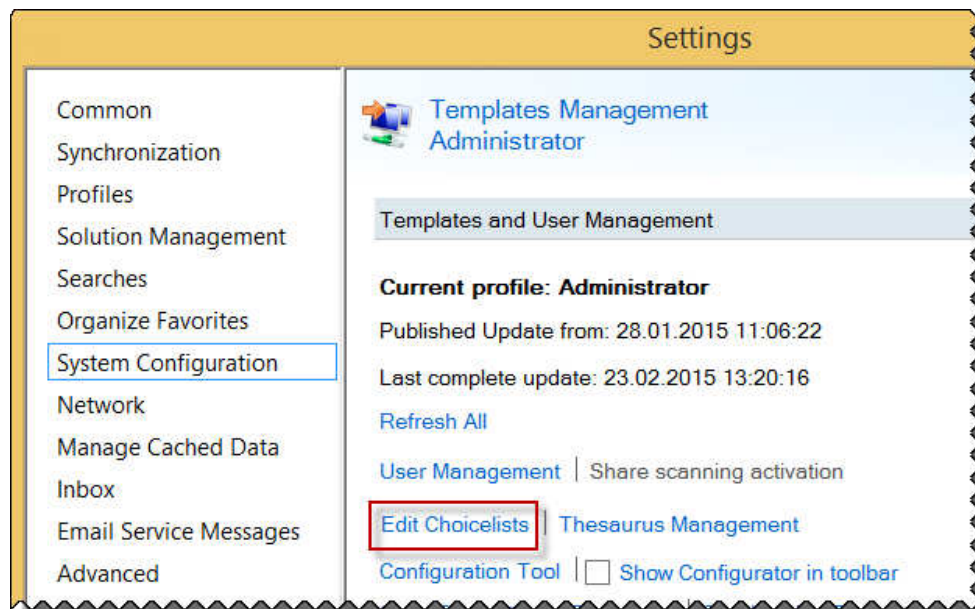
To find out which choice lists are available and the input screens in which they are used, please refer to the description for your solution.

---

### 13.4.2 Opening a choice list

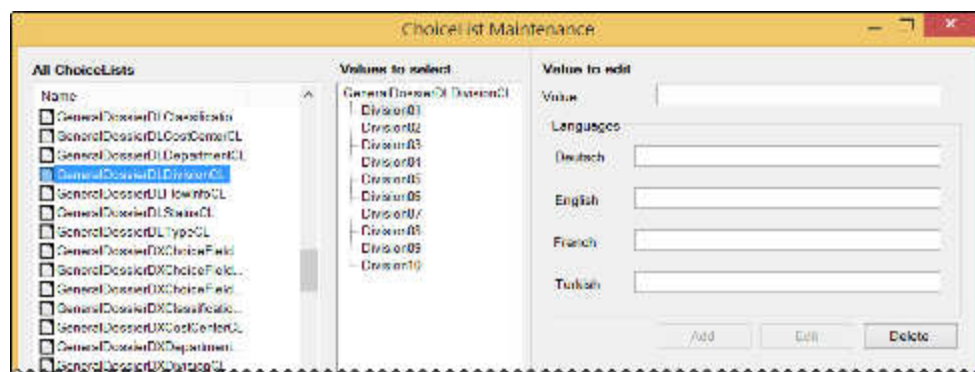
To open a choice list in order to edit it, follow the steps below:

1. Click on **Settings, System Configuration**. Then click on **Edit Choicelists**.



2. In the leftmost pane, select the choice list that you want to edit.

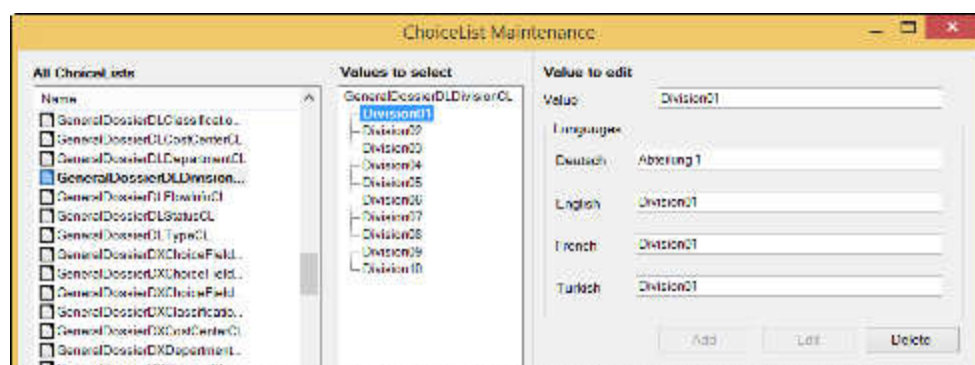
The pane in the middle will show the index values in that list.



### 13.4.3 Changing the label for an index value

To change an index value's label, follow the steps below:

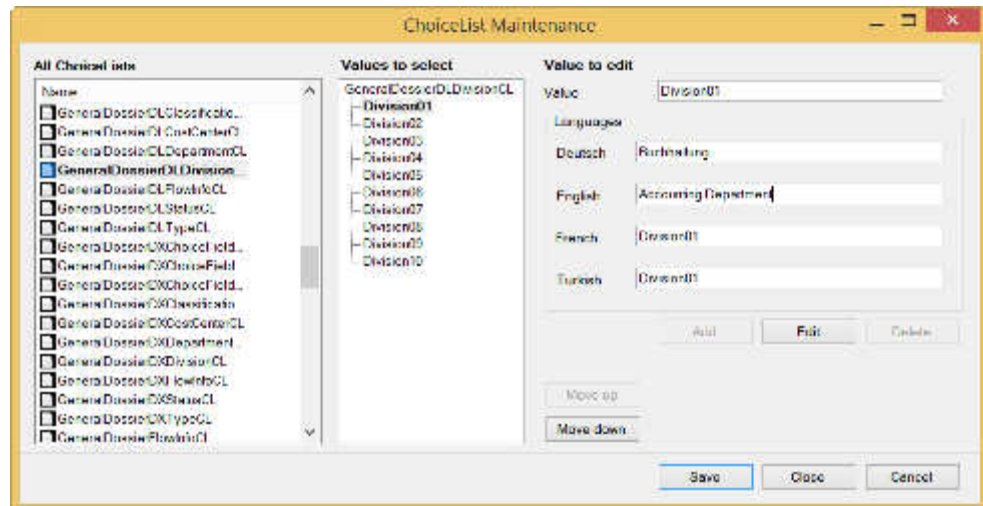
1. In the **Values to select** pane, select the index value for which you want to change the label.



The following will be shown under **Value to edit**:

- **Value** – (attribute value) The internal name that the system uses to identify which index value is being edited
  - **Languages** – The actual label that will be displayed, in various languages
2. Enter the label(s) you want into the corresponding **Languages** fields.

Click on **Refresh** to confirm the changes you have made.



3. To leave the dialog box, click on **Save** to confirm your changes.
4. To leave the dialog box, click on **Close** and then close the **Settings** dialog box by clicking on **OK**.

#### 13.4.4 Adding index values

Values (internal system values) must be unique within their choice list. Special characters (ä ö ü \* ? : < > \ /) are not permitted in these names. Before editing a choice list, make sure to become familiarized with the system being used for the corresponding values (it is recommended to keep using the same system). Moreover, before entering a value, make sure that it is not being used already. Please note:

---

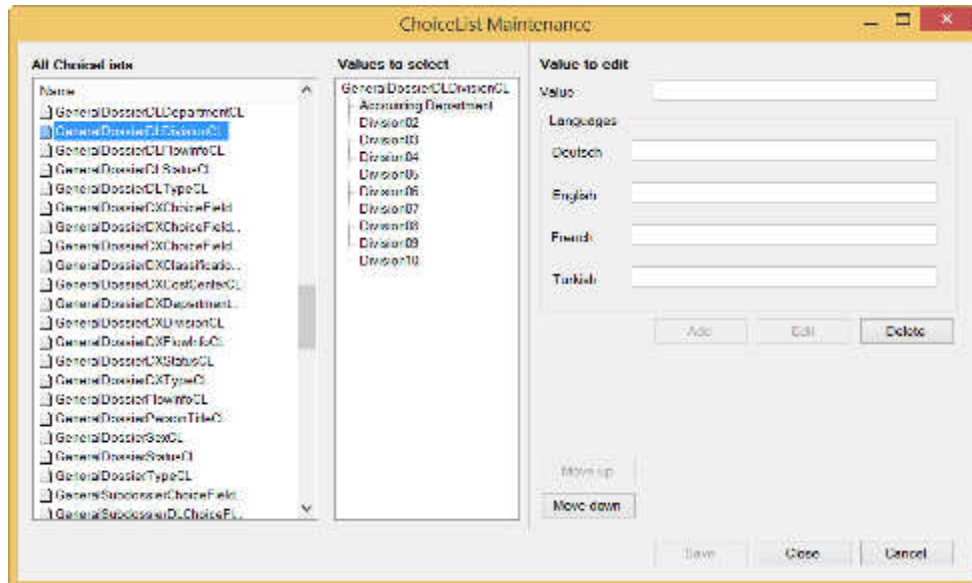
##### Please note:

For more information on the system and values used, please refer to the description for your solution.

---

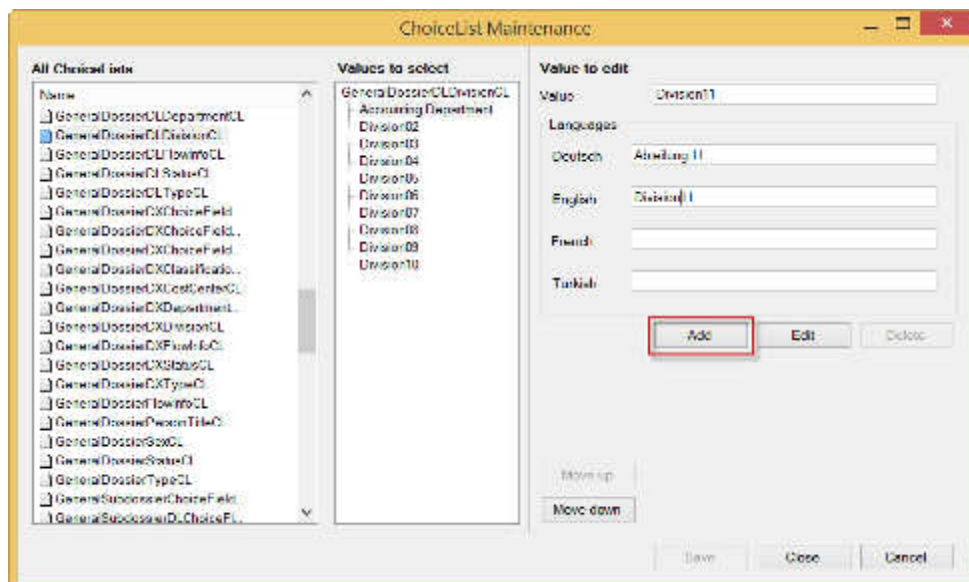
To add an index value to a choice list, follow the steps below:

1. Select the following as the starting point:
  - The name of the choice list, in the **All ChoiceLists** pane, if the list is a single-level choice list
  - The node to which you want to add the index value, in the **Values to select** pane, if the choice list is a cascaded choice list



2. Enter the value (internal system value) for the new index value into the **Value** field. Enter the label(s) you want into the corresponding Languages field(s). Then click on **Add**.

**Important:** If you are editing a single-level choice list, the **Value** field will be empty after you select the starting point. If you are editing a cascading choice list, the **Value** field will already be filled out. To add a new index value, overwrite the contents in the field.



3. To leave the dialog box, click on **Save** to confirm your changes. To leave the dialog box, click on **Close**.

### 13.4.5 Editing and adding nodes

Values (internal system values) must be unique within their choice list. Special characters (ä ö ü \* ? : &lt; &gt; \ /) are not permitted when naming values. Before editing a choice list, make sure to become familiarized with the system being used for the corresponding values (it is



recommended to keep using the same system). Moreover, before entering a value, make sure that it is not being used already.

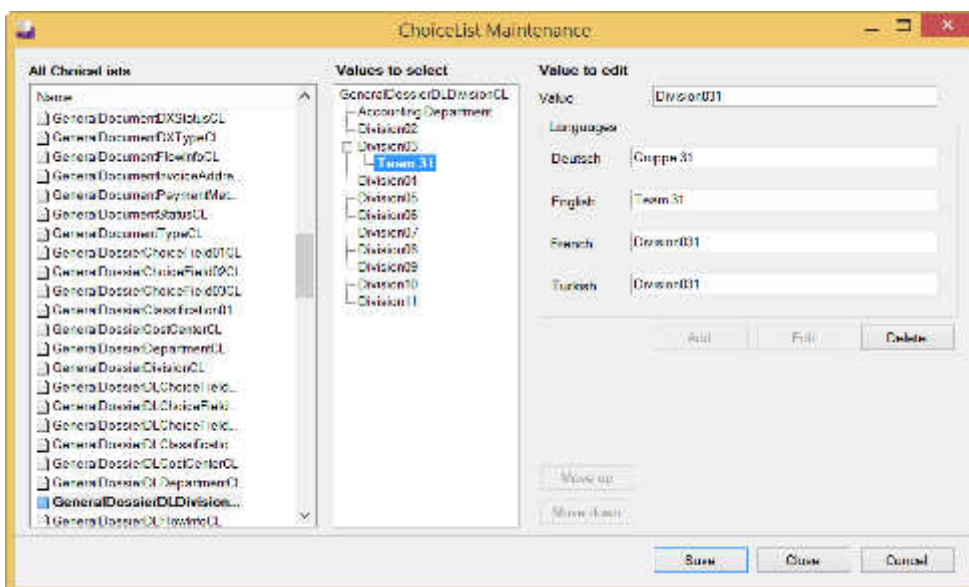
**Please note:**

For more information on the system and values used, please refer to the description for your solution.

You can add new index values to the nodes in a cascading choice list at any time.

Follow the steps below to add a new index value to a node:

1. In the **All ChoiceLists** pane, select the name of the choice list you want. In the **Values to select** pane, select the entry to which you want to add a new level.



2. Enter the value (internal system value) for the new sub-level entry (index value) into the **Value** field. Enter the label(s) you want into the corresponding **Languages** field(s). Click on **Add...**

**Important:** If you are editing a cascading choice list, the **Value** field will already be filled out. To add a new index value, overwrite the contents in the field.

3. To leave the dialog box, click on **Save** to confirm your changes. To leave the dialog box, click on **Close** and then close the **Settings** dialog box by clicking on **OK**.

**Tip:**

To change the order of the entries, use the **Move up and Move down** buttons.

Node labels can be changed. In addition, new index values can be added to nodes. Please refer to the **Adding index values** and **Changing the label for an index value** sections.

**Please note:**

If there is an existing index value and a sub-level with additional index values is added to it in the ChoiceList Maintenance dialog box, the original index value will become a node. Node labels cannot be used in the index fields for files, registers, or documents. If the label for an index value is already being used in files, registers, and/or documents before the change, the node's value will be shown. A new index value will have to be assigned to the corresponding index field.

### 13.4.6 Deleting index values and nodes

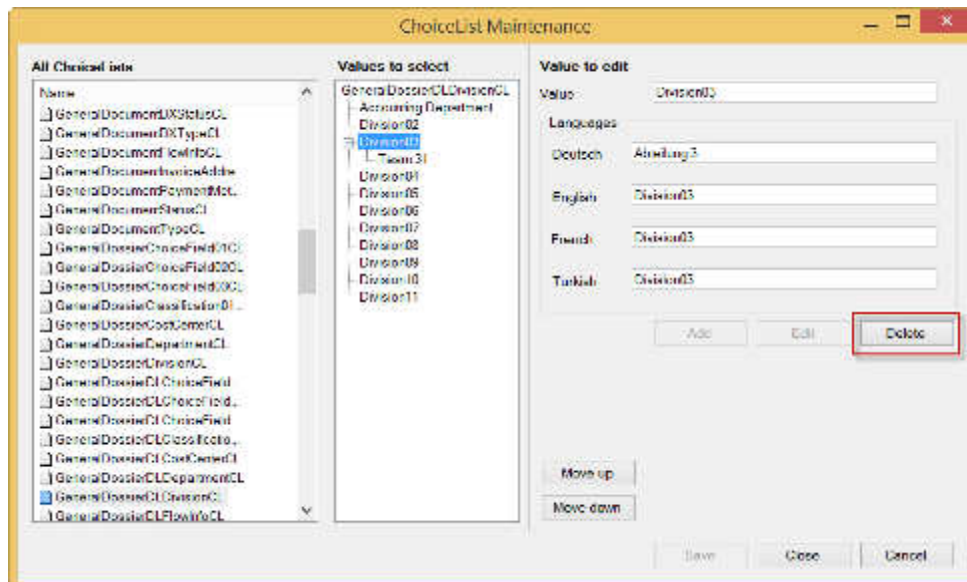
**Please note:**

It is recommended not to delete any index values or nodes before consulting with your solution vendor.

Index values and nodes can both be deleted.

To delete an index value or node from a choice list, follow the steps below:

1. In the **Values to select** pane, select the name of the index value or node you want to delete and click on **Delete**.



**Important:** When you delete a node, the entries underneath that node will also be deleted.

2. Click on **Save** to confirm the changes you have made. To leave the dialog box, click on **Close**.

**Please note:**

If the label for an index value is already being used in files, registers, and/or documents before the change, the index value's value will be shown after the index value is deleted. This also means that you will not be able to search for files, registers, or documents using the label anymore. A new index value will have to be assigned to the corresponding index field.

## 13.5 Updating templates

When it comes to templates that are locally stored on the filesystem, you can modify them yourself or send them to your solution vendor so that they can carry out a change request (custom update).

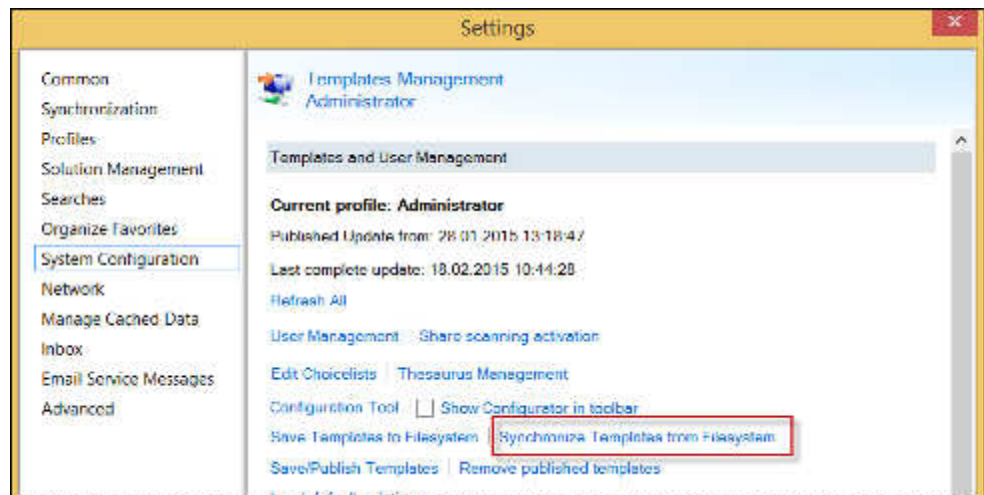
**Please note:**

Do not modify templates without first being briefed and trained by your solution vendor on how to do so. Improperly modifying templates may have a negative impact on the proper operation of the solution(s) installed for a tenant.

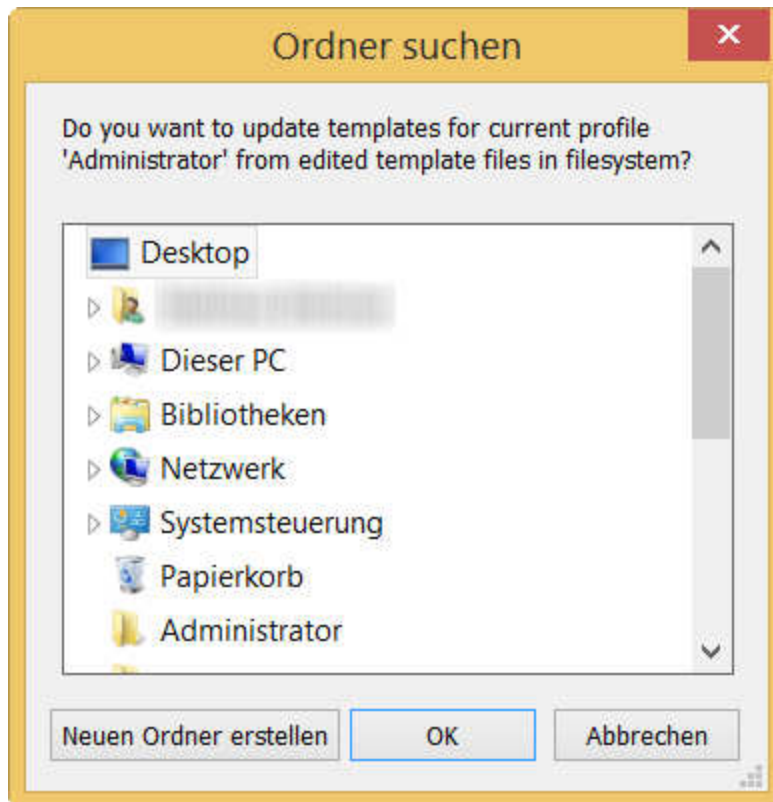
To transfer updated templates to doculife, use the **Synchronize Templates from Filesystem** function.

To transfer the updated templates, follow the steps below:

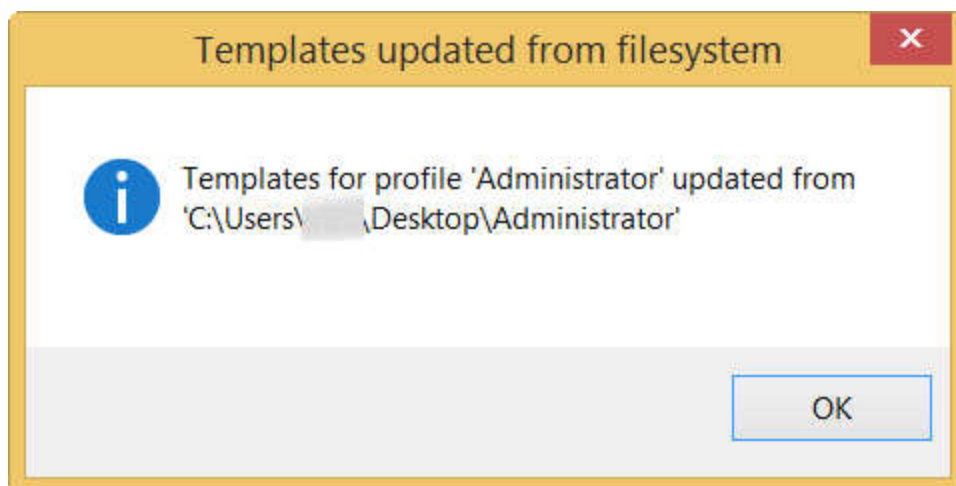
1. Click on **Settings, System Configuration**. Click on **Synchronize Templates from Filesystem**.



2. In the next dialog box, select a storage location for the updated templates and confirm your selection by clicking on **OK**.



3. In the prompt that appears, click on **OK**

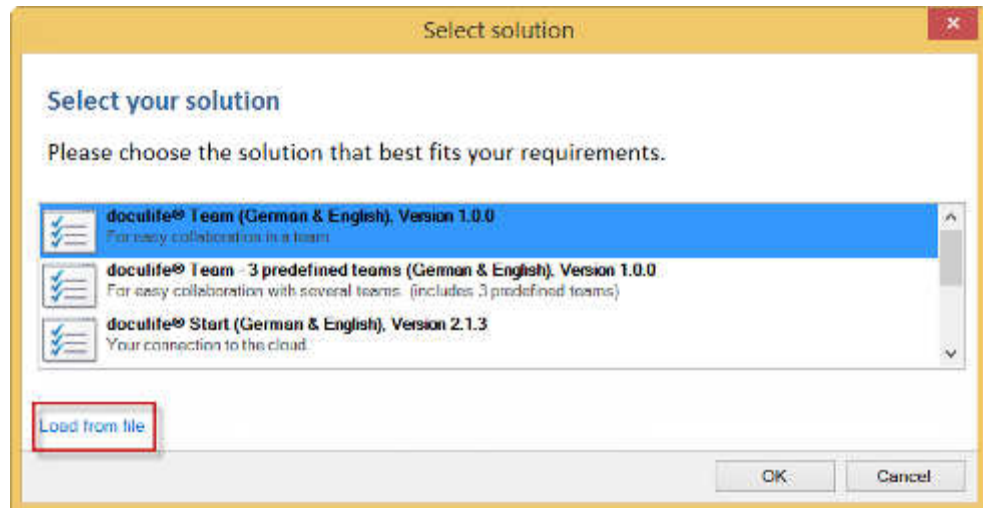


## 13.6 Solution updates

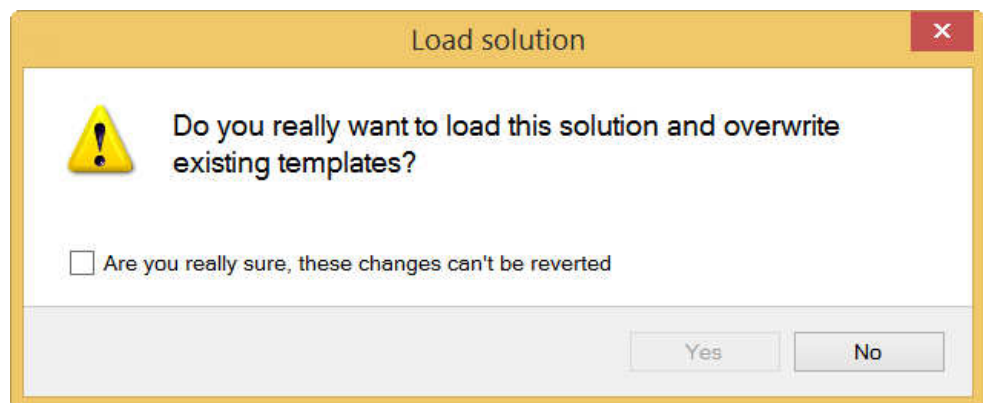
If you order updates or custom solutions from your solution vendor, the solution vendor will provide them in the form of a ZIP file (\*.zip).

To load a ZIP file (\*.zip), follow the steps below:

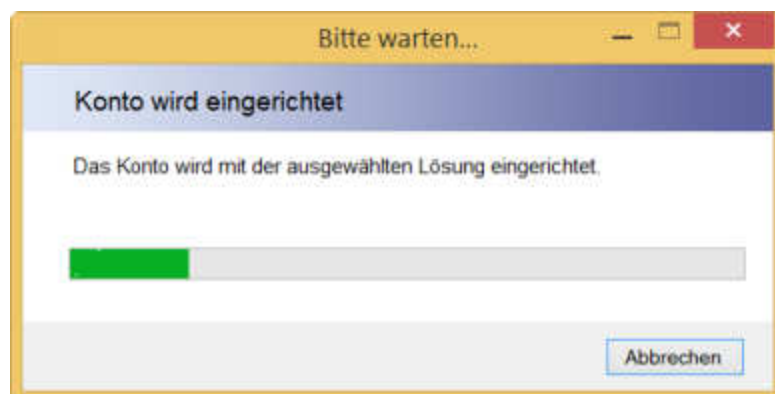
1. Click on **Settings, System Configuration**. Click on **Load solution**.
2. In the dialog box that appears, click on **Load from file**.



3. Select the solution's ZIP file (\*.zip) in the filesystem and start the loading process by clicking on **Open**.
4. Enable the checkbox next to "Are you really sure, these changes can't be reverted" Then click on **Yes**.



The solution will be loaded (this may take some time depending on how big it is).



5. Once the loading process is complete, close the **System Configuration** and **Settings** windows by clicking on **OK**.

**Important:** The settings will not be updated until users restart their Desktop. When they restart it, the settings will be automatically updated and the modified solution will be provided.

## 13.7 Saving and publishing changes

Only the administrator will be able to access the changes and additions you make to choice lists, searches, templates, and templates provided by your solution vendor after they are created / synchronized from the filesystem.

The administrator will be able to verify the corresponding choice lists, searches, and/or templates before the changes and/or additions are published. This ensures that it will be possible to make corrections without affecting users' work.

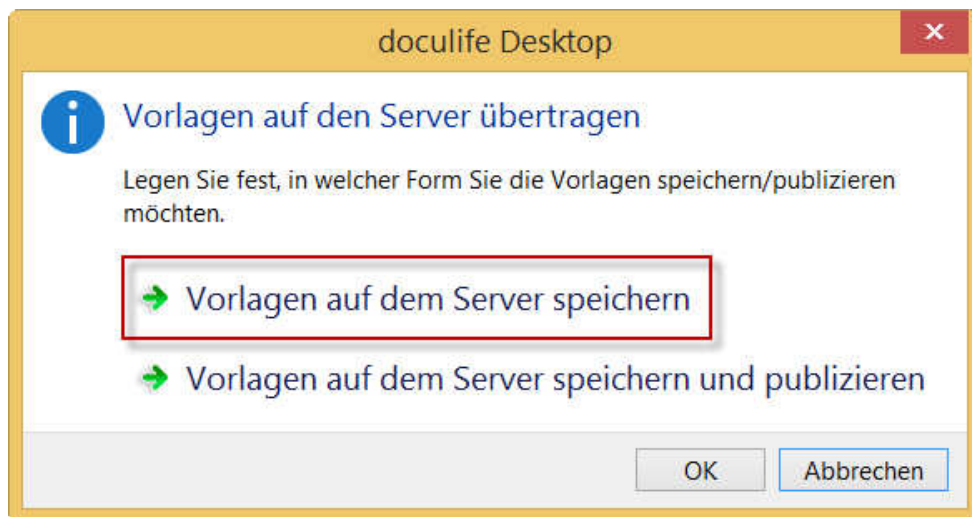
Changes and additions can:

- Be saved in doculife
- Be saved and published in doculife

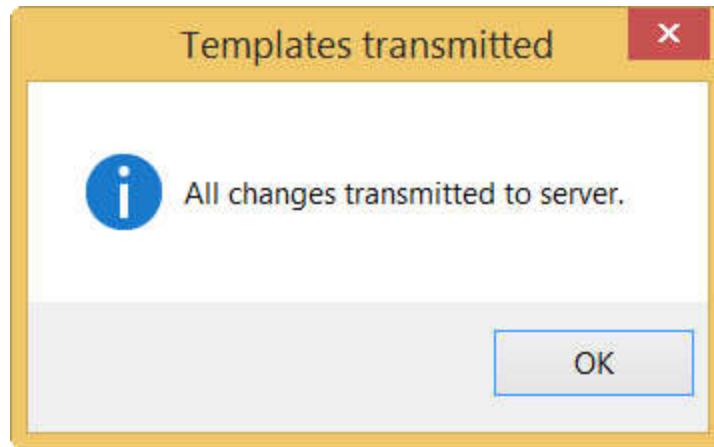
**Important:** Changes and additions will not be available to users until they are published.

To save changes and additions, follow the steps below:

1. Click on **Settings, System Configuration**. Click on **Save/Publish Templates**.
2. To simply save the changes/additions, click on **Save templates to server**.



3. The changes will be transferred to the server. In the prompt that appears, click on **OK**.

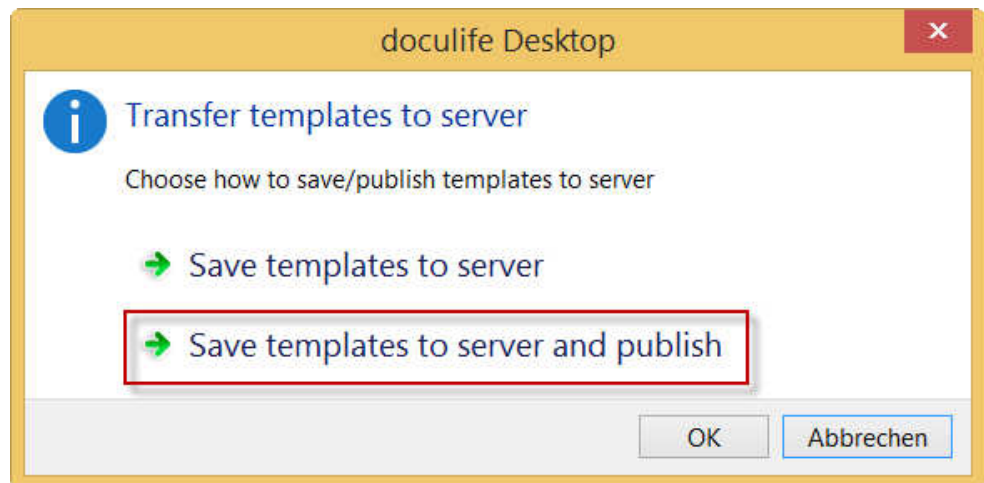


**Important:** The transferred changes will not be available to users until they are published.

4. Once you are done, close the **System Configuration** and **Settings** windows by clicking on **OK**.

To publish changes and additions, follow the steps below:

1. Click on **Settings, System Configuration**. Click on **Save/Publish Templates**.
2. To publish the changes/additions, click on **Save templates to server and publish**.



3. The changes will be transferred to the server and published. In the prompt that appears, click on **OK**.

**Important:** The settings will not be updated until users restart their Desktop. When they restart it, the settings will be automatically updated and the modified solution will be provided.

4. Once the loading process is complete, close the **System Configuration** and **Settings** windows by clicking on **OK**.

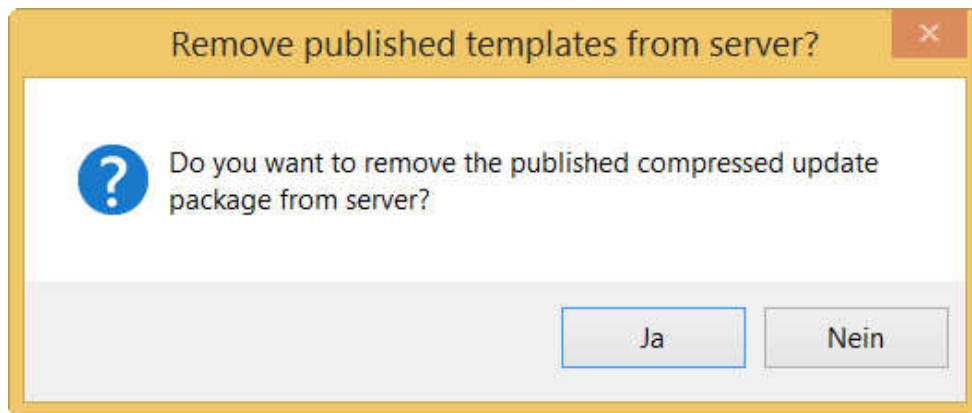
## 13.8 Revoking published templates

### Please note:

When published templates are revoked, all templates will be removed from your tenant and will cease to be available to users. To restore the tenant's proper functioning, you will need to load and publish the templates again. It is recommended to use this function only after consulting with your solution vendor.

To revoke published templates, follow the steps below:

1. Click on **Settings, System Configuration**. Select **Remove published templates**.
2. To remove the templates, click on **Yes** in the prompt that appears.



3. Once the process is complete, close the **System Configuration** and **Settings** windows by clicking on **OK**.

## 13.9 Feature set

### 13.9.1 Feature set overview

The feature set for a tenant can be customized as required for your company's specific needs. Among other things, the layout used for **My Workplace** and the range of functionalities in **Manage accounts...** can be configured as necessary.

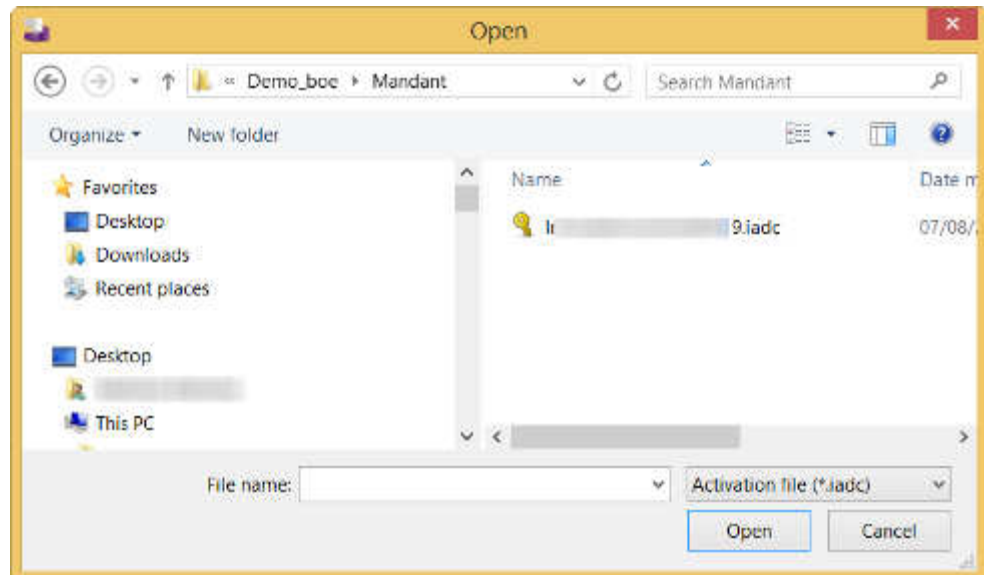
Feature sets will be provided by your solution vendor upon request.

### 13.9.2 Adding a feature set

Follow the steps below to add a feature set:

1. Click on **Settings, System Configuration**. Select **Add feature set for account**.
2. In the next dialog box, search for the location where the feature set (\*.idac) is stored. Select the feature set and click on **Open**.



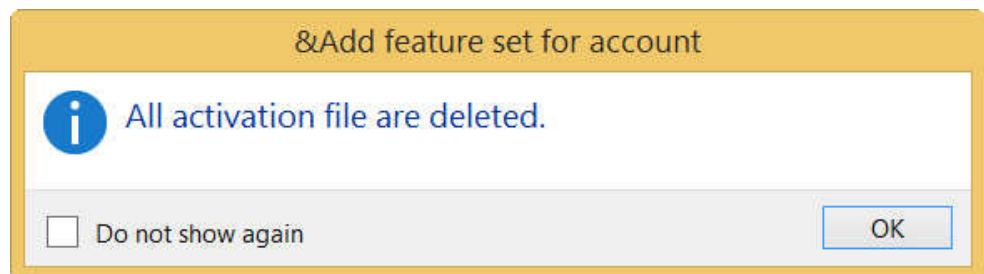


3. The configuration will be enabled After enabling the feature set, close the **System Configuration** and **Settings** windows by clicking on **OK**.

### 13.9.3 Feature set

Follow the steps below to remove a feature set and restore the corresponding default settings:

1. Click on **Settings, System Configuration**. Select **Delete feature set for account**.
2. In the prompt that appears, click on **OK**.



3. After removing the feature set, close the **System Configuration** and **Settings** windows by clicking on **OK**.

## 14 Audit

### 14.1 Overview

---

**Please note:**

Special administrator rights are required in order to be able to view an audit. Please make sure to observe your company's policies concerning access to confidential and personal data.

---

All actions concerning files, registers, documents, and user management in doculife are logged. These actions, which are also referred to as **events**, can be viewed by authorized users using WebClient.

The date and time, as well as the name of the user who performed the corresponding action, will be shown for each event. Events can be exported in the form of a CSV file (\*.csv).

In the case of files, some of the information that can be traced includes:

- Which user created or deleted a file and when
- Which user accessed a file and when
- Which user made changes to a file and when
- Which user changed the corresponding access permissions and when

In the case of registers, some of the information that can be traced includes:

- Which user created or deleted a register and when
- Which user accessed a register and when
- Which user moved a register and when
- Which user changed the corresponding access permissions and when

In the case of documents, some of the information that can be traced includes:

- Which user created or deleted a document and when
- Which user accessed a document and when
- Which user checked out a document or cancelled a checkout and when
- Which user created an attachment for a document and when
- Which user moved a document and when
- Which user changed the corresponding access permissions and when

In terms of user management, some of the actions that can be traced for specific users include:

- When a user was created, deactivated, reactivated, or deleted
- When a user was added to or removed from a group
- When management information was added to a user or modified for that user

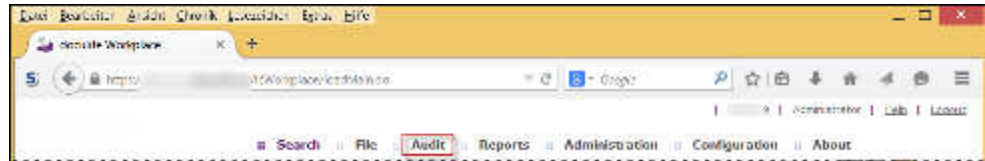
In addition, some of the information that can be traced for groups includes:

- When a group was created or deleted
- When a group was added to or removed from a group
- When management information was added to a group or modified for that group

## 14.2 Searching for events

To search for events, follow the steps below:

1. Open **WebClient** and click on the **Audit** tab.



2. Enter the search criteria you want into the Events search template and click on **Search**.

 A screenshot of the 'Search Mask: Events' search template. The form contains several input fields: 'Created (from):' and '(to):' with calendar icons; 'Title:', 'Dossier Name:', 'Action:', and 'User:' each with a magnifying glass icon; and 'DMS ID (Source):'. At the bottom, there is a 'Max. result:' dropdown set to '25', and three buttons: 'Search', 'Reset', and '<< Advanced Search'.

**Created (from) / (to):** The timeframe during which the event occurred

**Title:** The document's title

**Dossier Name:** The dossier's title

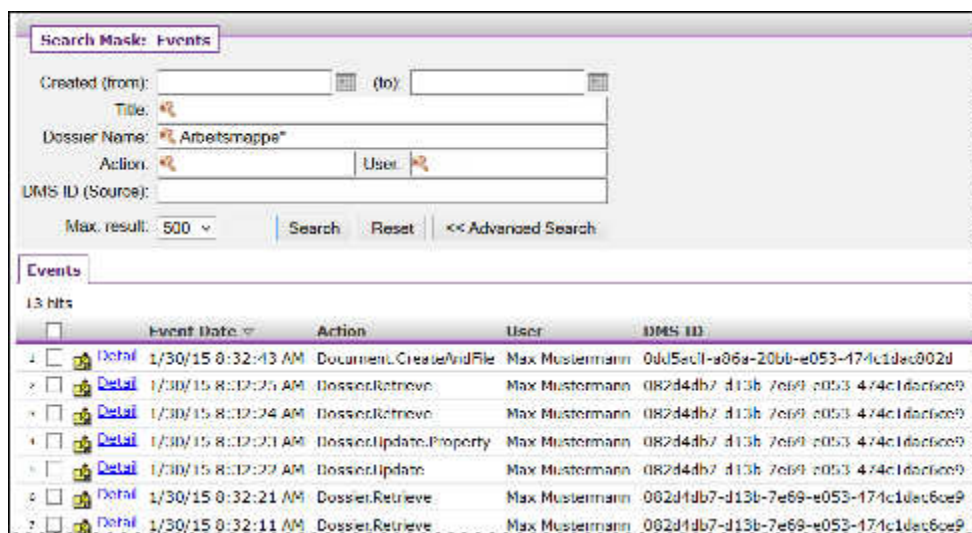
**Action:** The action's (event's) name

**User:** The name of the user who triggered the event

**DMS ID (Source):** The object's unique ID in doculife

**Important:** If you use the DMS ID criterion for your search, make sure to enter the full ID (e.g., 08068148-9a87-1c77-e053-474c1dacd3d3). In the case of documents, queries using the DMS ID will only return events for the documents' latest version. If you want the events to include events for versions, use the document name (Title) for your search.

The corresponding events will be shown.



By default, the hit list will show, for example, the date and name of the event, the name of the user who triggered the event, the DMS ID, the corresponding object name, and the old and new index values in an action-specific manner.

---

**Please note:**

To find out what the exact elements in the hit lists will be, please refer to the description for your solution. If you are interested in custom search templates and hit lists, please contact your solution vendor.

---

### 14.3 Calls for events

The following table lists all event calls that can be analyzed for files:

Name	Description
Dossier.Create	File created
Dossier.Delete.Request	File deletion confirmation prompt
Dossier.Delete	File deleted
Dossier.PrivilegedUsersUpdate	Not available by default
Dossier.Retrieve	File retrieved
Dossier.SecurityUpdate	File access permissions updated
Dossier.Update	File index values changed
Dossier.Update.Property	Changed file index values
Dossier.OwnerUpdate	File owner changed

The following table lists all event calls that can be analyzed for registers:

Name	Description
Folder.Create	Register created
Folder.Delete.Request	Register deletion confirmation prompt

Name	Description
Folder.Delete	Register deleted
Folder.Move	Register moved
Folder.Retrieve	Register retrieved
Folder.SecurityUpdate	Register access permissions updated
Folder.Update	Register index values changed
Folder.Update.Property	Changed register index values
Folder.OwnerUpdate	Register owner changed

The following table lists all event calls that can be analyzed for documents:

Name	Description
Document.Attachment	Attachment added
Document.CancelCheckout	Document checkout cancelled
Document.ChangeDossier	Document moved to dossier
Document.ChangeSecurityParent	New access permissions applied after moving the document
Document.Checkin	Document checked in
Document.Checkout	Document checked out
Document.Create	Document created
Document.CreateAndFile	File imported and document created
Document.Delete.Request	Document deletion confirmation prompt
Document.Delete	Document deleted
Document.File	Document was moved or linked
Document.PrivilegedUsersUpdate	Not available by default
Document.Retrieve	Document retrieved
Document.SecurityUpdate	Document access permissions updated
Document.Softdeleted	Document moved to Recycle Bin
Document.Unfile	Document link removed
Document.Update	Document index values changed
Document.Update.Property	Changed document index values
Document.Undelete	Document restored from Recycle Bin
Document.OwnerUpdate	Document owner changed

The following table lists all events that can be analyzed for user management:

Name	Description
UsersMgmt.Group.Attributes.Set	Management information set for group
UsersMgmt.Group.Create	Group created
UsersMgmt.Group.Delete	Group deleted
UsersMgmt.Membership.GroupGroups.Add	Group added to group
UsersMgmt.Membership.GroupGroups.Remove	Group removed from group
UsersMgmt.Membership.GroupUsers.Add	User added to group
UsersMgmt.Membership.GroupUsers.Remove	User removed from group
UsersMgmt.User.Attributes.Set	Management information set for user
UsersMgmt.User.Create	User created
UsersMgmt.User.Delete	User deleted
UsersMgmt.User.Disabled	User deactivated
UsersMgmt.User.Enabled	User reactivated
UsersMgmt.User.Locked	User locked
UsersMgmt.User.Password.Set	User password changed
UsersMgmt.User.Unlocked	User unlocked

## 15 Administration rights

### 15.1 Administrator

The **Administrator** user has all the permissions for managing the tenant and the solutions being used. In order to ensure that this user will be able to perform their administration tasks, they are a direct member of the following groups in doculife by default:

- AdminAccessG
- AdminOperationG
- BusinessUserG
- DisableSystemG
- LDAPAdminG
- StandardErrorInboxG
- StandardInboxG

---

**Please note:**

Do not change the groups to which the **Administrator** user is assigned as shown above, as doing so may mean that the permissions required for administrative tasks may not be fully available under certain circumstances.

---

If necessary, the **Administrator** user must be added to the following groups so that they will be able to use the corresponding Desktop functions:

- AdvancedTemplatesAdminG - Functions for saving templates on the filesystem and synchronizing template changes from the filesystem
- AdvancedLDAPAdminG - Function for deleting users and groups
- LibraryManagementG - Function for sharing libraries

---

**Please note:**

If the aforementioned groups are not created automatically when the solution is loaded, they will need to be created manually if required.

---

**Important:** In order to be able to customize the access permissions for files, registers, and documents, membership in the corresponding user groups will also be required in line with the permissions system.

### 15.2 Granting management permissions

The administrator can grant management permissions for administration functions to other users. To do this, the user needs to be added to the relevant groups.

Granting user management permissions

- LDAPAdminG - Grants permissions for managing all users and groups, resetting passwords, and sharing scanning activations
- LDAPBusinessAdminG - Grants permissions for creating users and groups, managing assigned users and groups, and sharing scanning activations

Granting editing permissions for choice lists

- ChoiceListAdminG - Grants permissions for editing choice lists

#### Granting managing permissions for templates

- TemplateAdminG - Grants permissions for saving and publishing templates, revoking published templates, loading solutions, and loading and removing feature sets

#### Granting permissions for viewing audits

- ViewAuditG - Grants permissions for viewing audits

#### Granting permissions for sharing libraries

- LibraryManagementG - Enables the function for sharing libraries

#### Granting permissions for viewing user access details

- BusinessInfoG - Grants permissions for showing all members with access to an object

#### Granting advanced administrator rights

- AdminOperationG - Grants permissions for managing technical groups, locking SECplus and SECmezzanine tenants, editing choice lists, saving and publishing templates, revoking published templates, loading solutions, loading and removing feature sets, archiving, and viewing audits

---

**Notes:**

Please refer to the description for your solution for more information on deviating assignments when granting management permissions

---



## 16 Index

<b>A</b>		<b>P</b>	
Audit		Passwords	
Events .....	76	guidelines .....	22
Overview .....	74	Resetting .....	24
Searching for events .....	75	Permissions concept	
<b>C</b>		Confidentiality levels .....	14
Choice lists .....	61	Data access and editing per- missions .....	14
Adding index values .....	63	Overview .....	14
Adding nodes .....	64	Permissions scheme .....	14
Changing the label for an index value .....	62	Permissions system	
Deleting an index value .....	66	Access permissions .....	15
editing .....	61	Personal inbox .....	51
<b>D</b>		Opening and working with .....	53
Direct user group		<b>R</b>	
Displaying group mem- berships .....	40	Register .....	10
Document .....	10	<b>S</b>	
<b>F</b>		Search	
Files .....	10	Creating .....	60
Finding documents .....	57	Making available to all users ..	60
Formatting and layout used throughout this doc- umentation .....	6	SECplus/SECmezzanine .....	45
<b>G</b>		Changing keys .....	48
General security information .....	7	Granting permissions for lock- ing a tenant .....	47
Group inbox .....	51	Locking tenants .....	45
Enabling .....	54	Sharing scanning activation files .	27
Opening and working with .....	55	Solution .....	9
Groups		Solution administration	
Deleting .....	44	Feature set .....	72
Permission groups .....	17	Loading a feature set .....	72
Technical groups .....	17	Overview .....	58
User groups .....	17	Publishing changes .....	70
Viewing permission groups ...	41	Removing a feature set .....	73
<b>I</b>		Revoking published templates	72
Inboxes		Saving templates .....	58
Adding to the inbox overview .	52	Solution updates .....	68
		Updating templates .....	67
		System configuration	
		Overview .....	11
		update settings .....	13
		System Configuration	
		Add-ins .....	13
		User management .....	11

---

**T**

Technical groups	
Overview .....	42
Technical user .....	16
Technical users	
Displaying .....	36
Technical Users	
Overview .....	35
Tenant .....	9

---

**U**

User	
Assigning management information .....	22
Editing user information .....	30
User types .....	22
User account	
Closing an account .....	31
Deleting .....	34
Reactivating .....	33
When to close an account .....	31
User group	
adding .....	37
Showing the members of a group .....	40
Users .....	16
Adding .....	18
Additional user account .....	28
Business users .....	16
Changing the groups for a user ..	26

## **OUR CONTACT DATA:**

Please call us.

Monday till Friday 9:00 a.m. – 5:00 p.m.

+49 351 4188 5841

Or write us to [doculife-support@mms-support.de](mailto:doculife-support@mms-support.de)

**T · · Systems ·**