

ArchiveKeeper User Manual

Version: 1.0

Date: 09.12.2024



COMPRISE GmbH

www.comprise-world.com | archivekeeper-support@comprise-world.com



Content

1.	About this manual	1
1.1	Target group	1
1.2	Terms and symbols	1
2.	Validity	2
3.	Release notes	2
4.	What is ArchiveKeeper?	2
5.	Introduction to audit-proof archiving	2
5.1	Advantages of ArchiveKeeper	3
5.2	Basic concept	3
5.2.1	Functions	3
5.2.2	The user interface	3
5.2.3	Authorization concept	5
5.2.4	Security	8
5.2.5	Standards	9
5.2.6	Expandability	9
5.3	Introduction of ArchiveKeeper	9
5.3.1	System requirements	9
5.4	Working with ArchiveKeeper	9
5.4.1	Data protection	9
5.5	First steps with ArchiveKeeper	9
6.	PART I: Using ArchiveKeeper	9
6.1	Basics document space and documents	9
6.1.1	Document space overview	10
6.1.2	Document space actions User	10
6.1.3	Document space details	10
6.1.4	Documents	10
6.1.5	Document upload	11
6.1.6	Document search	13
6.1.7	Document Actions	13
6.1.8	Wastebasket	18
6.2	Administrative management	19
6.2.1	The document space	19
6.2.2	The metadata schema	23
6.2.3	Users	31
6.2.4	Groups	33
6.2.5	Roles	35

6.2.6	Translations	37
-------	--------------------	----

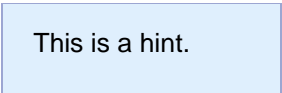
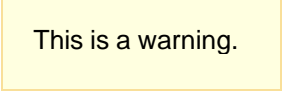

1. About this manual

1.1 Target group

This manual is intended for end users of ArchiveKeeper who wish to use this application.

1.2 Terms and symbols

Term	Description
Document Space/DocSpace	Delimited area in which documents are stored. This area is used to define metadata, Retention period, access rights and revision safety
Metadata	Metadata is structured data that contains comprehensive information about a resource - such as books, web documents, videos or images.
Metadata schema	Schema in which individual metadata is defined. A metadata schema is assigned to a document space. When uploading to this document space, metadata can be filled depending on the valid schema.
Document version	Documents cannot be edited (traceability, revision safety). However, new versions can be created where a modified/new document has been uploaded or changes have been made to the metadata. Each version is logged and can be traced retrospectively
Retention period	Period in which a document must be retained (legal requirement). This is defined in ArchiveKeeper at document space level
Revision safety/ Audit-proof	Data or documents are stored and managed in such a way that they remain unchangeable and traceable to ensure reliable verifiability
Deletion concept/deletion mode	Differentiation between physical and logical deletion. Individual definition per document space
Logical deletion	A document is not actually deleted, but only made invisible to the user (moved to the recycle bin)
Physical deletion	A document is also deleted from the memory with restrictions. Note: However, deletion only takes place after 2 days, before that it is only marked for deletion and is no longer visible to users. Restriction: Residual data that is stored to ensure revision safety (applies in audit-proof document spaces and for metadata that has been defined as audit-proof)

Icon	Description
	Information/Note.
	This symbol indicates important aspects to be considered.
	Indicates a function that is not included in the standard scope and requires an additional license.

2. Validity

This installation description is valid for the following versions of ArchiveKeeper:

- ArchiveKeeper 2.2
- ArchiveKeeper 2.3
- ArchiveKeeper 2.4
- ArchiveKeeper 2.5

3. Release notes

Version	Changes
1.0	Initial Version

4. What is ArchiveKeeper?

ArchiveKeeper is an audit-proof cloud archive. Users can add individual metadata to their documents and store them in secure document spaces. The documents can be found easily at any time using the metadata and document names. This archive supports users with access management for each document space, compliance with the retention period, the definition of various deletion options, versioning and much more to ensure revision safety and easy document management.

5. Introduction to audit-proof archiving

The term is based on the understanding of auditing from a business perspective and relates to information and documents that must be retained or are worthy of retention. This means, among other things, that no manipulation is possible, changes are created and logged as new document versions, there is defined role and authorization management, and security standards are adhered to.

The following features therefore apply to audit-proof archives:

- **Completeness:** No document must be lost on the way to the archive.
- **Immutability:** All documents are archived unchanged and in principle unchangeable. However, changes can be made by creating new versions. Both the current and older versions can be accessed retrospectively.
- **Regularity:** Each document must be stored in accordance with legal and internal organizational guidelines.
- **Retrievability:** All information must be retrievable, for example by indexing with metadata.
- **Use only by authorized persons:** All information must be archived in such a way that it can only be viewed by authorized persons.
- **Protection against loss:** Data security must be guaranteed at all times.
- **Observe retention periods:** A document may be deleted from the archive at the earliest when its retention period has expired.
- **Documentation:** Detailed documentation of the archiving process is mandatory, for example to enable a smooth migration of the archive.

- **Traceability:** All changes in the archive must be logged so that they can be traced and the original status can be restored.
- **Verifiability:** An audit-proof archive system must be verifiable by a third party expert at any time.

ArchiveKeeper combines revision safety with maximum user-friendliness.

5.1 Advantages of ArchiveKeeper

The strength of ArchiveKeeper lies in the large number of individual configuration options. Admin users can define metadata for the document spaces themselves. Data types, restrictions (selection options), searchability, encryption, mandatory fields, revision safety and much more can be set individually. A new metadata schema can also be assigned at a later date (subject to the restriction that the integrity remains intact). Different document spaces can have different metadata schemas and also different Retention periods. Furthermore, non-audit-proof document spaces can also be created for other documents that are not subject to retention in order to have a central storage location available. No (potentially costly) changes by the software manufacturer are necessary for all these settings; instead, users can configure the product independently with regard to metadata and document spaces based on their needs.

Thanks to the cloud solution, employees can access it from anywhere and the available storage space can easily be changed at a later date.

5.2 Basic concept

5.2.1 Functions

- Document spaces
- Metadata schemas
- Central authorizations: Admin and additionally definable roles (e.g. only for read authorizations)
- Groups & Users
- Search functions

5.2.2 The user interface

5.2.2.1 Navigation

The individual menu items of ArchivKeeper are listed vertically on the left. The view differs depending on the assigned authorizations.

The different settings can be found under [Authorization concept](#)

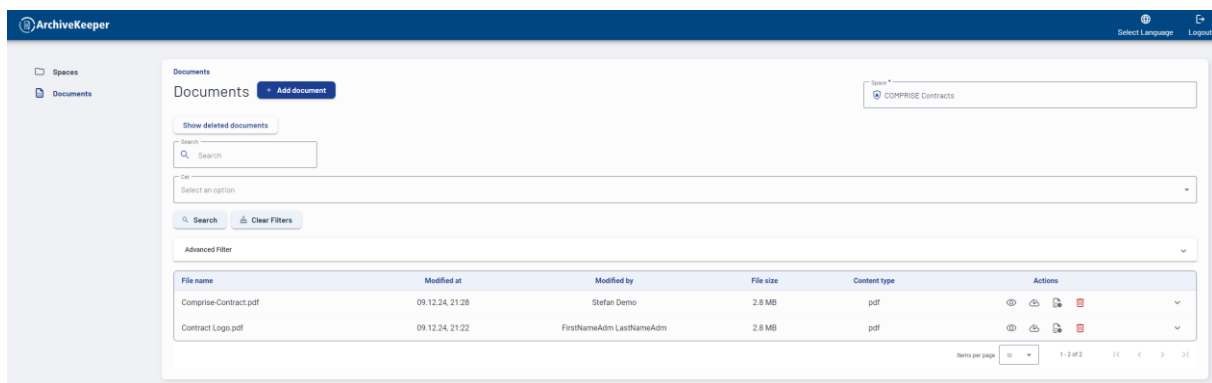
5.2.2.2 Menu top right corner

- Selecting the language
- Log out

5.2.2.3 Standard user view

Three areas are available to the standard user (no central authorizations): Start, document spaces and documents.

- Start: Page with basic information
- Document spaces: Overview of all document spaces for which the user is authorized.
 - The user can use actions to go directly to the documents or view the document space details
 - The settings that have been defined for the respective document space can be viewed in the document space details (name, schema, audit-proof, encryption, deletion concepts, retention period, etc.).
- Documents: Documents can be viewed, downloaded or deleted here for each authorized document space (depending on the Retention period and deletion concept of the document space).
 - Furthermore, general document information (including metadata) and the various versions can be called up in the document details.
 - Click on the document to display the metadata as a submenu.

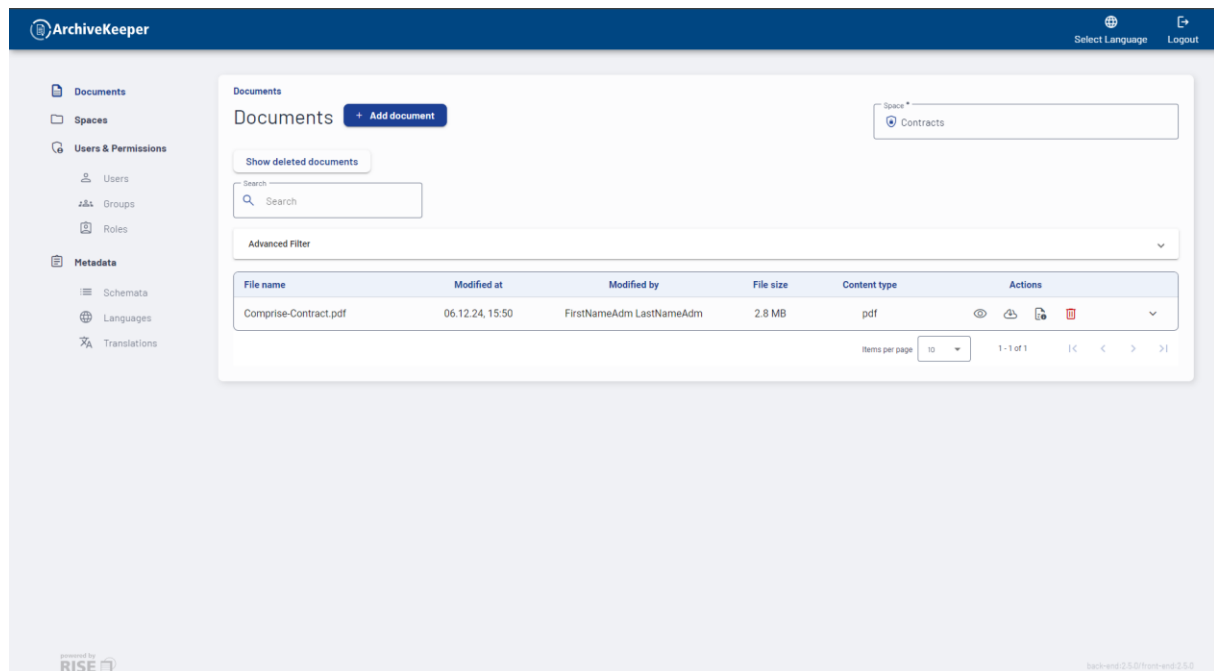


5.2.2.4 Admin user view

In addition to Start, Documents, Document spaces, the following administrative areas are available to the admin user: Users, Groups, Document spaces, Schemas, Roles

- Document spaces: document spaces can be created or deleted with central authorizations, an existing document space can be used as a template for creating a new one
- Users: Overview and information on all users, editing, deleting and deactivating individual users, creating new users
- Groups: Overview of all groups, group details action, delete groups, create new groups
 - Group details: overview, add or remove users, change document spaces and the authorization (read, edit, delete) of users in this document space or define new ones

- Schemas: creation of new metadata schemas, deletion of existing schemas, schema details with the individual metadata fields, an existing metadata schema can be used as a template for creating a new one
- Roles: Overview of roles (admin, support, etc.), creation of new roles with assignment of central authorizations, deletion of roles (admin is automatically created again) Role details
 - Role details: overview (ID and description), add or remove rights



5.2.3 Authorization concept

5.2.3.1 Groups and users

ArchiveKeeper has groups with assigned users. The users can be created in the administration area. Any number of document spaces can be assigned to each group. The following rights are defined for each document space: read, write, logical deletion, physical deletion and deletion in storage for the respective group.

5.2.3.1.1 Read

If only this right is selected, only read actions are possible. If other actions are selected, the Read permission is also automatically selected.

As soon as a group is assigned to a document space, the Read permission is therefore always assigned as the minimum permission

5.2.3.1.2 Writing

This right allows you to add documents and create new versions.

5.2.3.1.3 Logical Delete

Delete permission to move files to the recycle bin. Logical deletion is only permitted if this deletion mode has been defined as permitted in the document space.

5.2.3.1.4 Physical Delete

Delete permission to permanently delete files. However, this permission can only be used to delete files that are no longer within the retention period. Physical deletion is only permitted if this deletion mode has been defined as permissible in the document space.

5.2.3.1.5 *Force Delete*

With this deletion permission, it is possible to delete files that are still within the retention period. When this deletion is carried out, additional reasons must be given as to why the deletion is being carried out within the retention period; this is documented in the audit logs and is retained even after the document deletion.

However, this is only possible if the physical deletion mode is permitted in the document space.

5.2.3.2 **Document space access**

This concept means that users in a group only have access to certain document spaces (e.g. delimitation of a department or between document spaces that are only relevant for certain professional groups) and only have defined rights for these document spaces. (e.g. group A can only read in document space A1, group B can read, write and delete in document space A1 and can read and write in document space B1)

This concept thus makes it possible to distinguish between different operating sites, organizations, professional groups and hierarchical levels.

5.2.3.3 **Roles**

A flexible role and authorization system has been introduced in this application. Roles are specific collections of authorizations that are used to grant certain global access rights.

5.2.3.3.1 *Modifiability of roles*

Roles are not fixed, but can be modified. This means that

- **Create:** You can add new roles based on specific authorization requirements.
- **Update:** You can adjust the authorizations of a role as required.
- **Delete:** Roles can be removed (with the exception of the Admin role, which always has all authorizations and must always remain)

5.2.3.4 Authorizations/Permissions

Permissions are internal authorizations (e.g. DOCSPACE_CREATE - right to create the document space) that apply system-wide and therefore do not relate to individual document spaces. These authorizations are assigned to the corresponding roles.

Selected authorizations with their effects:

- **API_ACCESS**
 - To be able to use ArchiveKeeper, each user must have the API_ACCESS authorization. This authorization can be contained in one or more roles, but it must be present.
- **DOCSPACE_SEARCH**
 - Authorization to search for all DocSpaces available in the ArchiveKeeper → Menu item Document spaces is displayed and to see DocSpace details
- **DOCSPACE_CREATE**
 - Create a new DocSpace incl. assignment of a schema
- **DOCSPACE_DELETE**
- **DOCSPACE_UPDATE**
- **DOCSPACE_READ**
 - View documents in a DocSpace
- **GROUP_SEARCH**
 - Search for all groups → Groups menu item is displayed
- **GROUP_CREATE**
 - Create a group without assigning users and individual document spaces
- **GROUP_DELETE**
- **GROUP_USER_ASSIGN**
 - Assign users to a group
- **GROUP_USER_UNASSIGN**
 - Remove users from a group
- **GROUP_ACL_CREATE**
 - Assign DocSpaces to a group
- **GROUP_ACL_DELETE**

- Remove DocSpaces from a group
- **USER_CREATE**
- **USER_DELETE**
- **USER_EDIT**
- **USER_SEARCH**
 - Search for all users in ArchiveKeeper → Users menu item is displayed
- **DOCUMENTS_PRUNE**
 - Permanently (physically) delete documents
- **METADATA_SCHEMA_CREATE**
- **METADATA_SCHEMA_DELETE**
- **BINARY_READ**
 - Enables documents to be viewed
- **ROLE_CREATE**
- **ROLE_DELETE**
- **ROLE_UPDATE**
- **ROLE_READ**
 - Read all roles in ArchiveKeeper → menu item Roles is displayed
- **PERMISSION_READ**
 - Read permission details

5.2.3.5 Example of a role with corresponding authorizations:

A person responsible for controlling should have access to all of the company's document spaces, but should not be able to upload documents or make changes to metadata schemas or document spaces. This person is therefore only given global read authorizations, e.g: API_ACCESS, DOCSPACE_SEARCH, DOCSPACE_READ, BINARY_READ.

For example, if this person is also assigned to a group that has all group rights in the Controlling document space. This person can perform all actions in this specific document space.

5.2.4 Security

ArchiveKeeper ensures security and encryption using the following methods:

- Transport encryption between all services - data is only transported from and to storage in encrypted form

- A separate key is used per document space for symmetric encryption of the data
- Key management using KMS with SoftwareSecureModule (SSM) backend
- Integration of a rekeying mechanism to always use current and valid algorithms and prevent compromising

5.2.5 Standards

Audit security is based on the specifications of TR-ESOR of the BSI (BSI TR-03125 preservation of evidence of cryptographically signed documents).

5.2.6 Expandability

The REST APIs enable integration into other existing systems

Individual offers can be made for customizations outside the standard configurations.

5.3 Introduction of ArchiveKeeper

5.3.1 System requirements

Docker must be installed for your own operation.

Otherwise, there are no system requirements as the application is called up via the browser.

5.4 Working with ArchiveKeeper

- Use as a central archive system with easy-to-find documents
- Use to fulfill requirements according to GoBD , GAAP, HRMC etc.
- Use to fulfill other legal requirements (audit proof, retention periods)
- Use as file storage for an external system

5.4.1 Data protection

Access authorizations and encryption concept prevent unauthorized access to data

Possibility to encrypt sensitive data space or to encrypt individual metadata (with personal data).

5.5 First steps with ArchiveKeeper

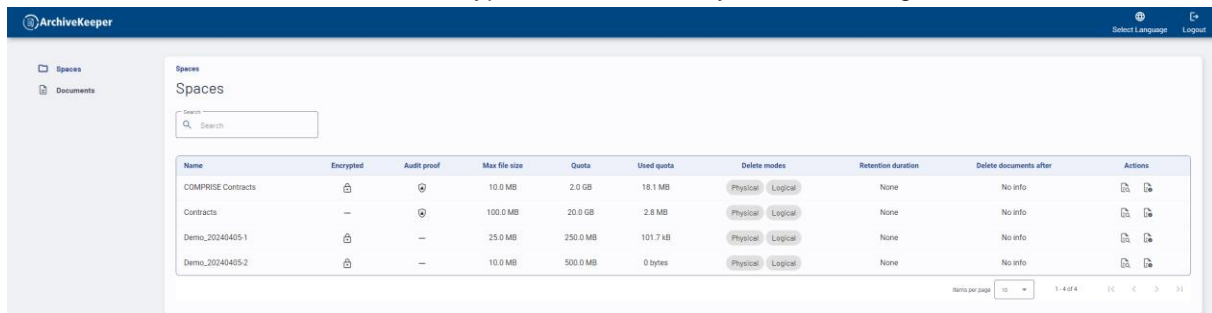
On the following pages you will find detailed documentation on all ArchiveKeeper functions. The successful introduction of ArchiveKeeper in your company is now up to you. Start with training in small teams and organize the introduction step by step without overburdening them. The enthusiasm of your colleagues will then be as expected and guarantees further motivation to use ArchiveKeeper.

6. PART I: Using ArchiveKeeper

6.1 Basics document space and documents

6.1.1 Document space overview

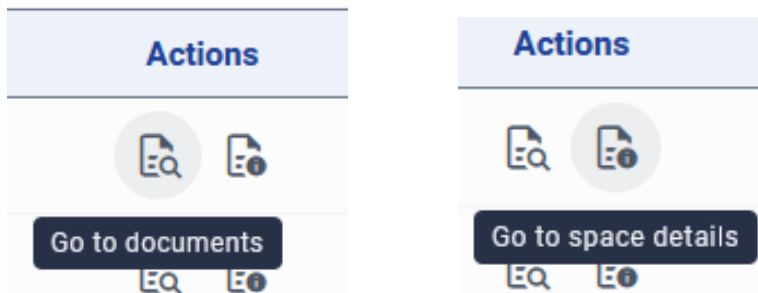
All document spaces assigned to the user can be seen in the Document spaces area. The overview contains basic information such as encryption, revision safety, retention obligation, etc.



Name	Encrypted	Audit proof	Max file size	Quota	Used quota	Delete modes	Retention duration	Delete documents after	Actions
COMPRISE Contracts			10.0 MB	2.0 GB	18.1 MB	Physical Logical	None	No info	
Contracts	—		100.0 MB	20.0 GB	2.8 MB	Physical Logical	None	No info	
Demo_20240405-1		—	25.0 MB	250.0 MB	101.7 kB	Physical Logical	None	No info	
Demo_20240405-2		—	10.0 MB	500.0 MB	0 bytes	Physical Logical	None	No info	

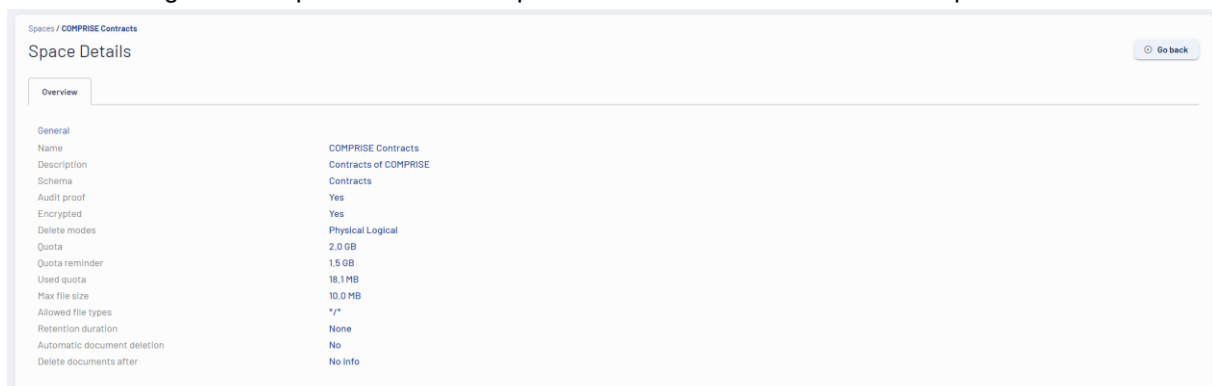
6.1.2 Document space actions User

In the document space overview, users without additional authorization can either go directly to the document space documents or view the document space details.



6.1.3 Document space details

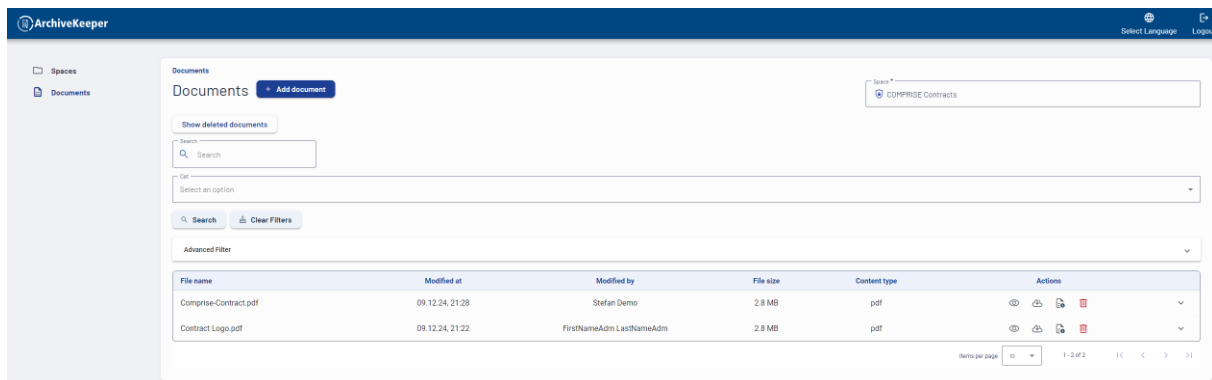
Further settings for the specific document space can be found in the document space details.



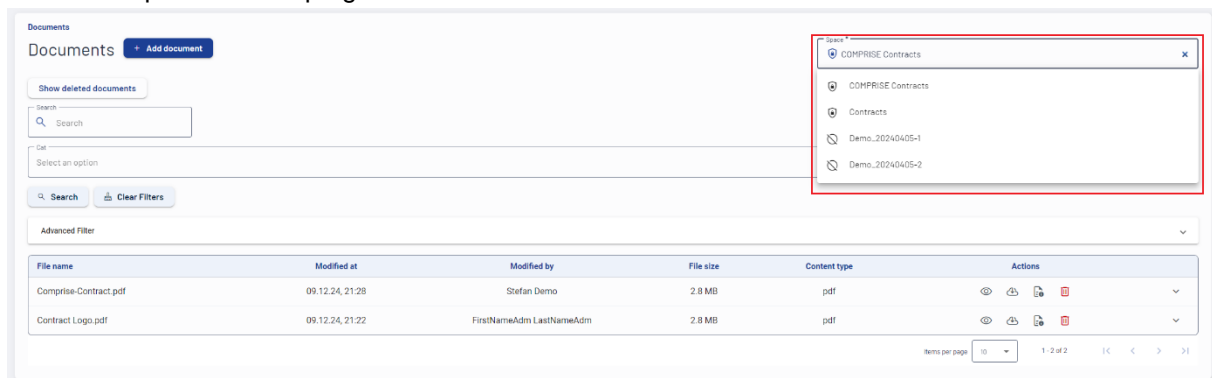
Spaces / COMPRISE Contracts	
Space Details	
Overview	
General	
Name	COMPRISE Contracts
Description	Contracts of COMPRISE
Schema	Contracts
Audit proof	Yes
Encrypted	Yes
Delete modes	Physical Logical
Quota	2.0 GB
Quota reminder	1.5 GB
Used quota	18.1 MB
Max file size	10.0 MB
Allowed file types	*/*
Retention duration	None
Automatic document deletion	No
Delete documents after	No info

6.1.4 Documents

By clicking on "Go to documents", the individual documents of the document space appear and further documents can be stored.



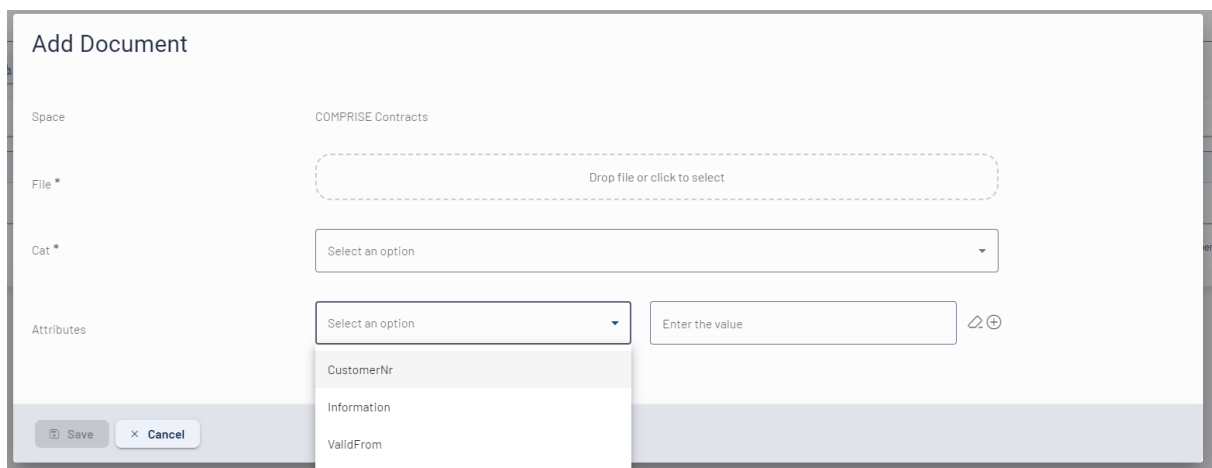
You can also switch directly to other document spaces from this page. To do this, select the desired document space in the top right-hand corner.



6.1.5 Document upload

Files can be uploaded to the selected document space using the "Add document" button.

Basic configurations, such as retention period, possible file types, etc., are regulated via the document space.



The file can be dragged and dropped in or selected directly from the file system. In addition to the file, the individual metadata can be filled in.

Mandatory fields are marked with an asterisk. Optional metadata fields can be selected and filled in under Attributes.

The schemas are defined individually and assigned to the document spaces. The upload screen and the possible metadata therefore look different depending on the schema of the document space.

Add Document

Space: COMPRISE Contracts

File *: Comprise-Contract.pdf

Cat *: Supply contract

Attributes: ValidFrom 24.12.2024 📅 🔗 + Add attribute

💾 Save ✕ Cancel

Add Document

Space: COMPRISE Contracts

File *: Comprise-Contract.pdf

Cat *: Supply contract

Attributes: ValidFrom 24.12.2024 📅 ⊖
Information test 🔗 ⊖ + Clear attribute

💾 Save ✕ Cancel

Add Document

Space: COMPRISE Contracts

File *: Comprise-Contract.pdf

Cat *: Supply contract

Attributes: ValidFrom 24.12.2024 📅 ⊖
Select an option Enter the value 🔗 ⊖ + Remove attribute

💾 Save ✕ Cancel

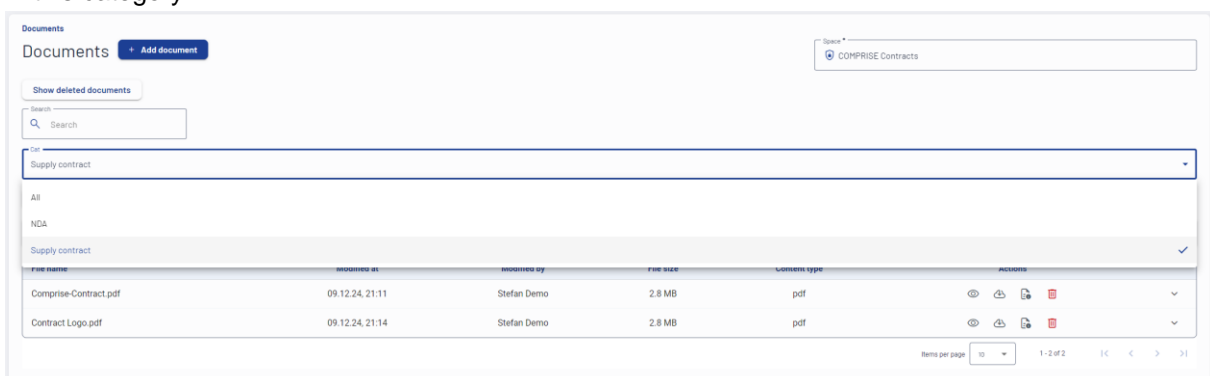
To the right of the attribute, you can use the symbols to add more (plus), remove the respective field (minus) or delete only the content (eraser symbol) of the current field.

6.1.6 Document search

The search and filter function can be used to find relevant documents and information more quickly in the document space.

The view of the search and filter mask and the searchable metadata depend on the metadata schema of the document space and therefore differ from that shown in the image. What is included in the full text search is also defined in the schema.

In the images shown below, the "Category" metadata field is filtered first. Two documents can be found in this category.



The search is then refined by entering the text "Logo" in the general search field. This will display the document that contains the term "logo" in the information.

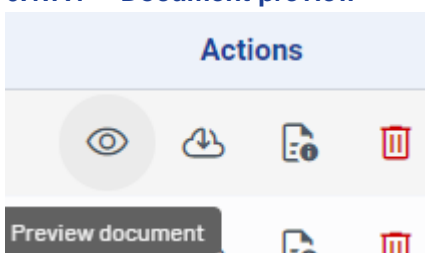
This image also shows that clicking on the respective line of the document displays the assigned metadata.



6.1.7 Document Actions

Various actions are available to the user for each document

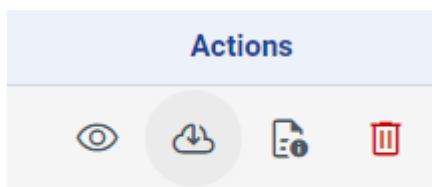
6.1.7.1 Document preview



Documents can be viewed here in advance (without downloading). The view is noted in the version log. However, the preview function is not available for all file formats.

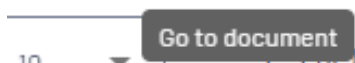
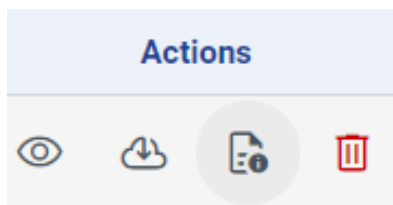


6.1.7.2 Download documents

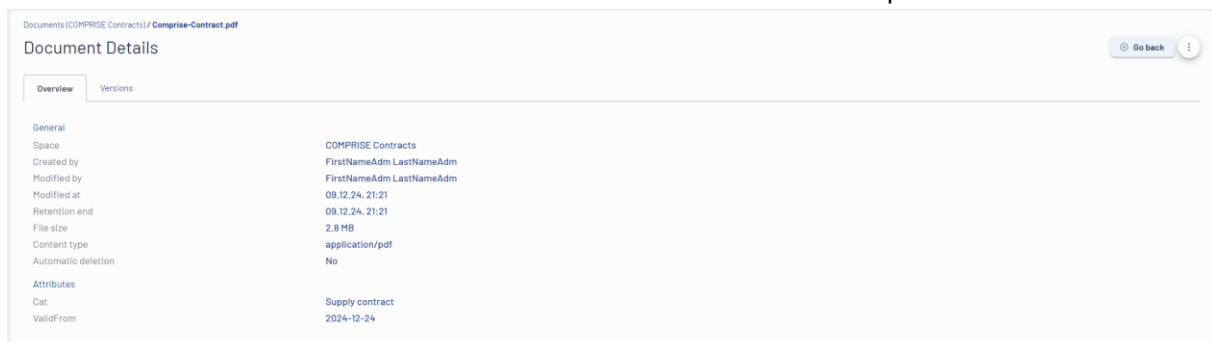


Documents are saved to the local device with this action. This action is also noted in the version log.

6.1.7.3 Document details



Further information on the document and the individual versions can be requested here.



All metadata can be seen in the document details overview.









General metadata refers to standard data such as file name, creation date, etc. This data is saved with every file. Attributes are the metadata defined in the metadata schema.

Documents[COMPRISE Contracts] / Comprise-Contract.pdf

Document Details

Go back

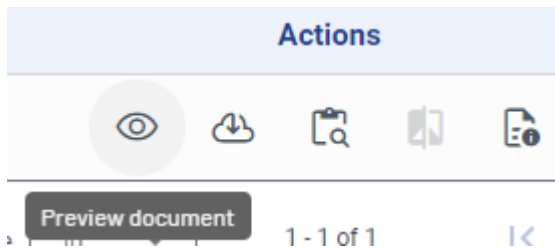
Overview Versions

Version	File name	Content type	Created at	Created by	Actions
1	Comprise-Contract.pdf	application/pdf	09.12.24, 21:28	Stefan Demo	   
Original	Comprise-Contract.pdf	application/pdf	09.12.24, 21:21	FirstNameAdm LastNameAdm	   

Items per page 10 1 - 2 of 2

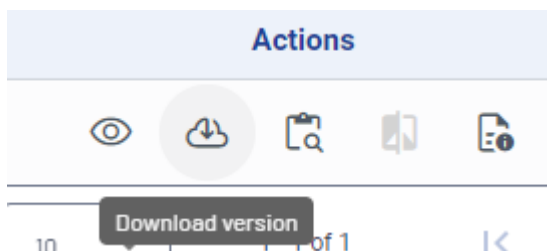
The individual versions are shown in the Versions tab and actions are possible for each version.

6.1.7.3.1 Preview



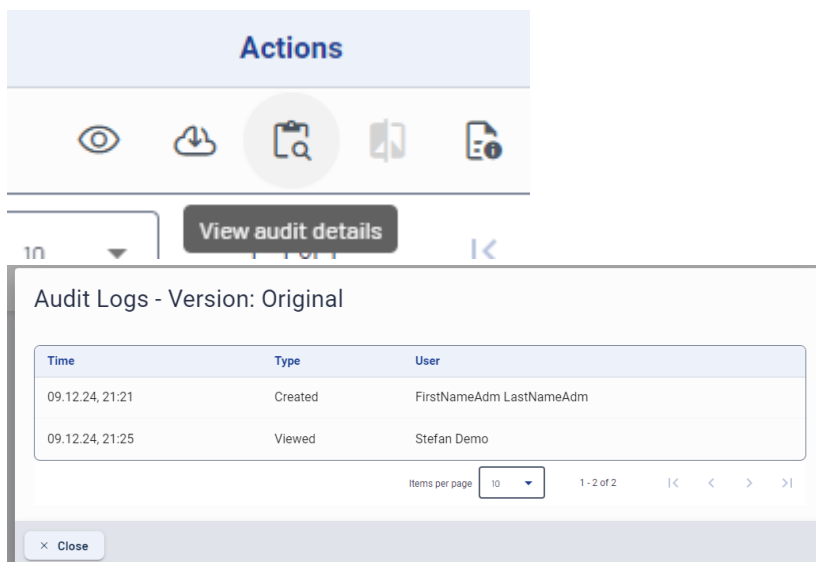
As in the general document view, the content of the selected version is displayed here as a preview.

6.1.7.3.2 Download



As in the general document view, the file of the selected version is also downloaded here.

6.1.7.3.3 Protocol



Audit Logs - Version: Original

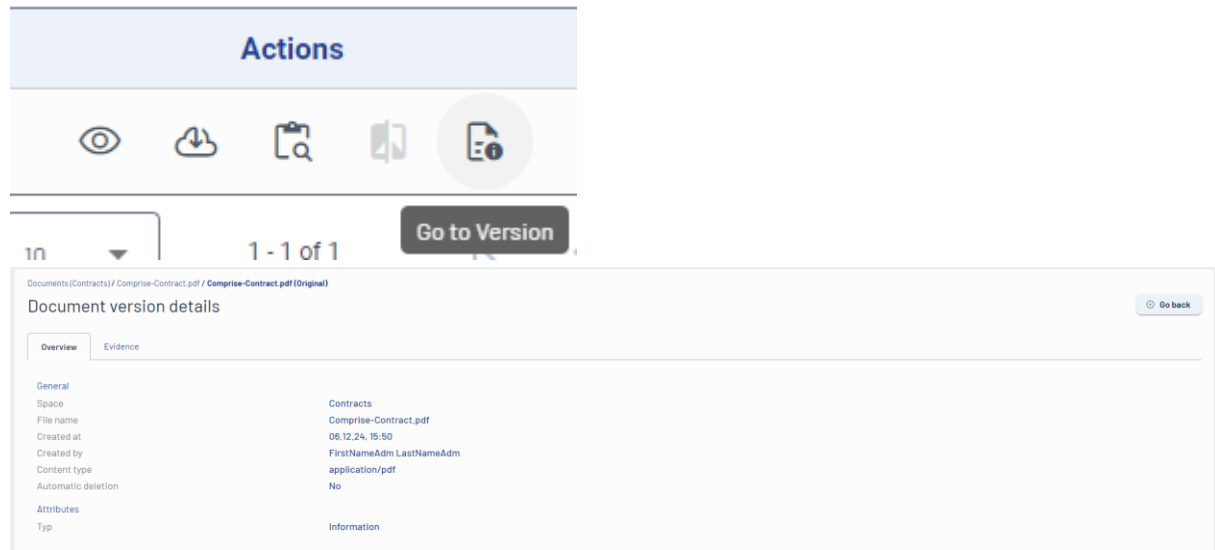
Time	Type	User
09.12.24, 21:21	Created	FirstNameAdm LastNameAdm
09.12.24, 21:25	Viewed	Stefan Demo

Items per page 10 1 - 2 of 2

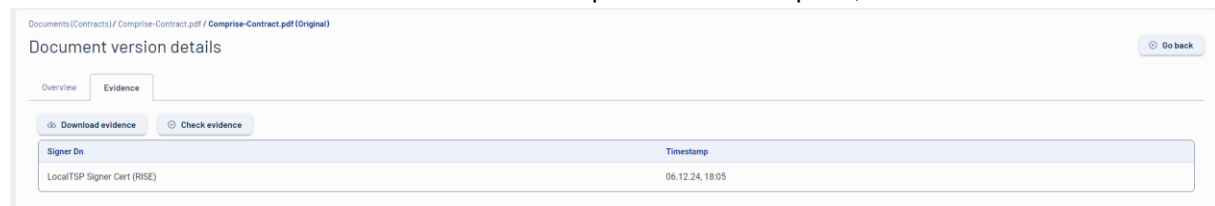
Close

The version log contains all changes and actions of the selected version

6.1.7.3.4 Version details



Clicking on "Continue to version" takes you to the detailed information for the selected version. The general and schema-specific metadata can be seen in the Overview tab. For documents that have been stored in an audit-proof document space, there is also the Evidence tab.

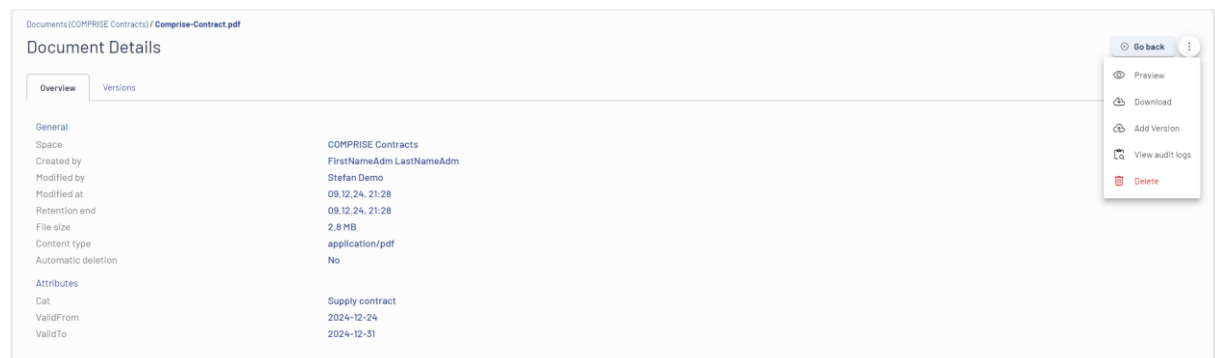


The signature can be checked here. The overview shows the name of the signature and the timestamp with which the revision was signed.

The time of this time stamp does not correspond to the time of creation, as documents are sent collectively to the time stamp service.
By default, the time stamp is generated max. 2 hours after creation.

The download button can be used to download an XML file containing more detailed information on the revision evidence.

6.1.7.3.5 Further actions Document details

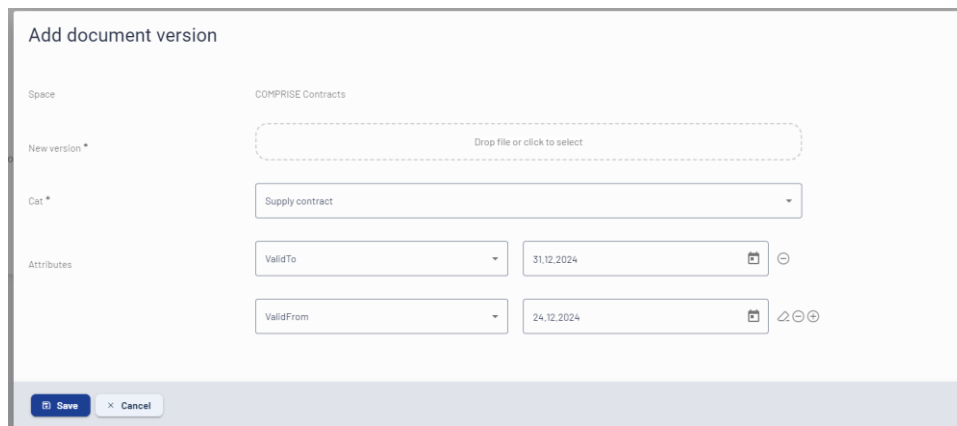


Various actions are also possible in the document detail view. These can be selected by clicking on the three dots in the top right-hand corner and selecting the desired action.

The following actions are possible here:

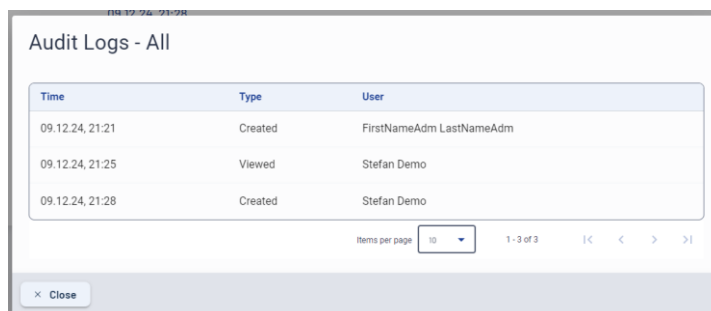
- **Preview:** As in the general document view, the content of the current version is displayed here as a preview.

- Download: As in the general document view, the file of the current version is also downloaded here.
- Add new version
 - This action can be used to save a new file or new, modified metadata as a new version of the document.
 - If no new document is uploaded and only the metadata is changed, the stored document remains valid for the new version. It is therefore not necessary to upload the same document again if only metadata is to be changed



If a new version is stored, the Retention period applies from the creation date of the new version. Example: Document A has been stored for 9 years and 11 months and the Retention period is 10 years, so it would be possible to delete the document in one month. A new file is now uploaded (via the "Add new version" action). The document can now only be physically deleted after 10 years from the current date.

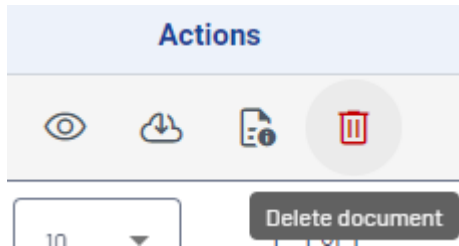
- Version audit logs: The version log contains all changes and actions of all document versions



Time	Type	User
09.12.24, 21:21	Created	FirstNameAdm LastNameAdm
09.12.24, 21:25	Viewed	Stefan Demo
09.12.24, 21:28	Created	Stefan Demo

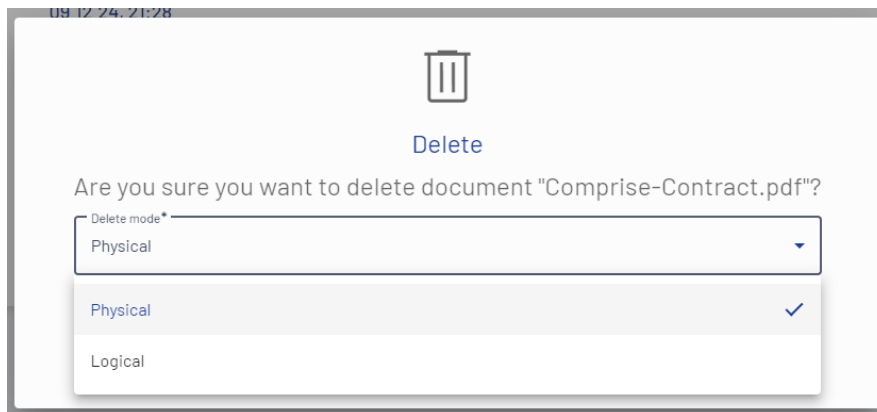
- Delete: Here, as in the general document view, you can delete a document (with all versions possible) For more information, see [Delete document](#)

6.1.7.4 Delete document

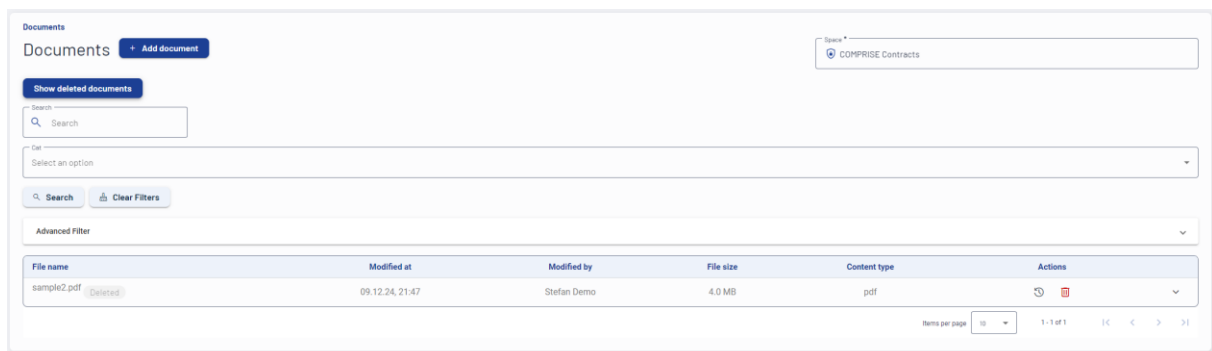


This action cannot be used to delete a document. Which deletion mode is used is defined in the document space.

- If only logical deletion is possible in the document space, the document is moved to the recycle bin.
- If only physical deletion is possible in the document space, the document is physically deleted. Relevant residual data for ensuring revision safety is retained. In addition, deletion within the system only takes place after a time limit has expired (2 days)
- If both deletion modes are defined in the document space (logical and physical). When you click on the "Delete document" action, a pop-up window appears in which you can select the desired mode.



6.1.8 Wastebasket



The "Show deleted documents" button takes you to the recycle bin. All logically deleted documents are displayed here.

The deleted documents can also be restored from the recycle bin.

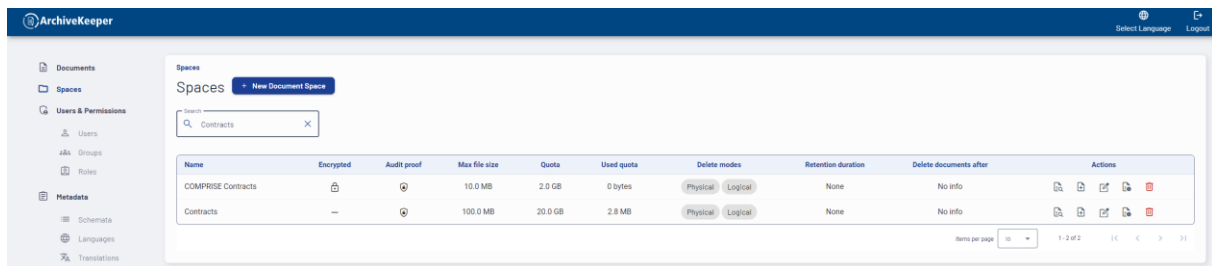
6.2 Administrative management

6.2.1 The document space


Document spaces can be viewed, edited, created and deleted in the Document spaces area.

Deletion is only possible if no groups have been assigned to the document space. Attention Default groups that are automatically assigned must be removed before deletion.

Only users with appropriate central authorizations can make changes to document spaces.



6.2.1.1 Create document space

A document space can be created from scratch (New document space button) or an existing one can be used as a template ( icon under Actions).

Prerequisite: a suitable metadata schema has been created beforehand.

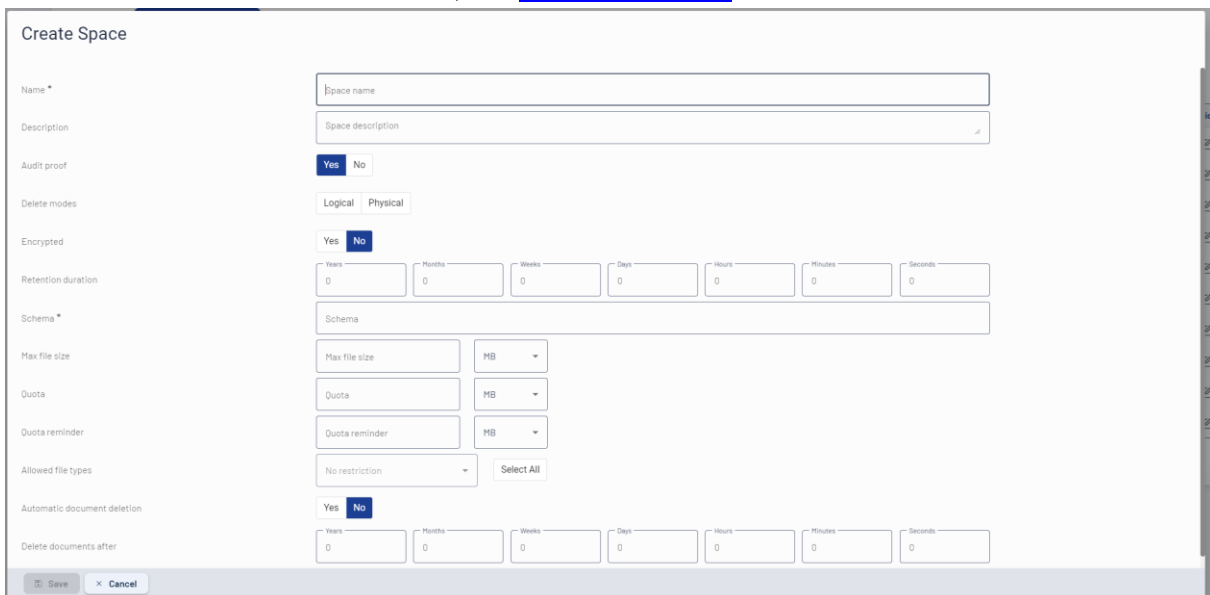
A number of settings can be made when creating a document space.

The name of the document space must be unique. Entering a description can be very useful, as the description is included in the search for document spaces.

This means that the document space "X1234" with the description "Accounting for location 1" is also found with "Location 1".

Previously created metadata schemas can be selected for the schema. If encryption is provided for certain metadata in the schema, the document space must also be encrypted.

For further details on schema creation, see [Metadata schema](#)



Create Space

Name *

Description

Audit proof ☒ Yes ☐ No

Delete modes ☐ Logical ☐ Physical

Encrypted ☒ Yes ☐ No

Retention duration
 Years Months Weeks Days Hours Minutes Seconds

Schema *

Max file size MB

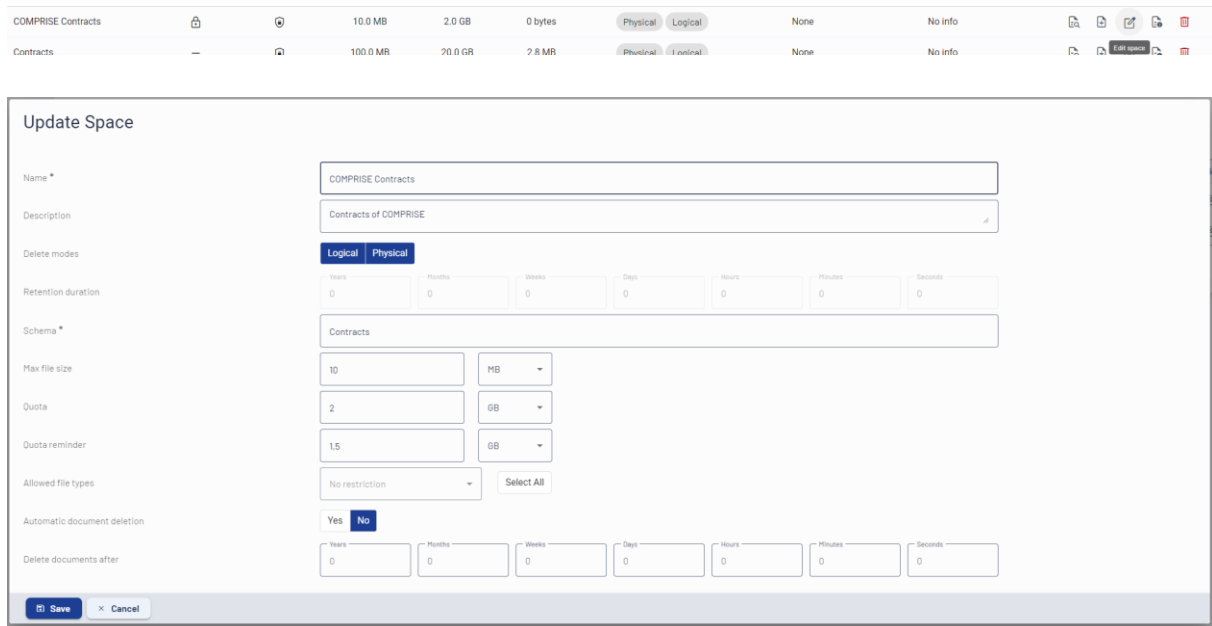
Quota MB

Quota reminder MB

Allowed file types

Automatic document deletion
 Years Months Weeks Days Hours Minutes Seconds

6.2.1.2 Edit document space



Update Space

Name *

Description

Delete modes **Logical** **Physical**

Retention duration
 Years Months Weeks Days Hours Minutes Seconds

Schema *

Max file size

Quota

Quota reminder

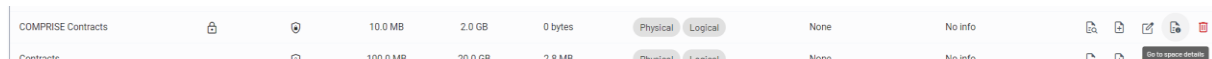
Allowed file types

Automatic document deletion
 Delete documents after Years Months Weeks Days Hours Minutes Seconds

The document space settings can generally be changed at a later date, but the following restrictions apply:

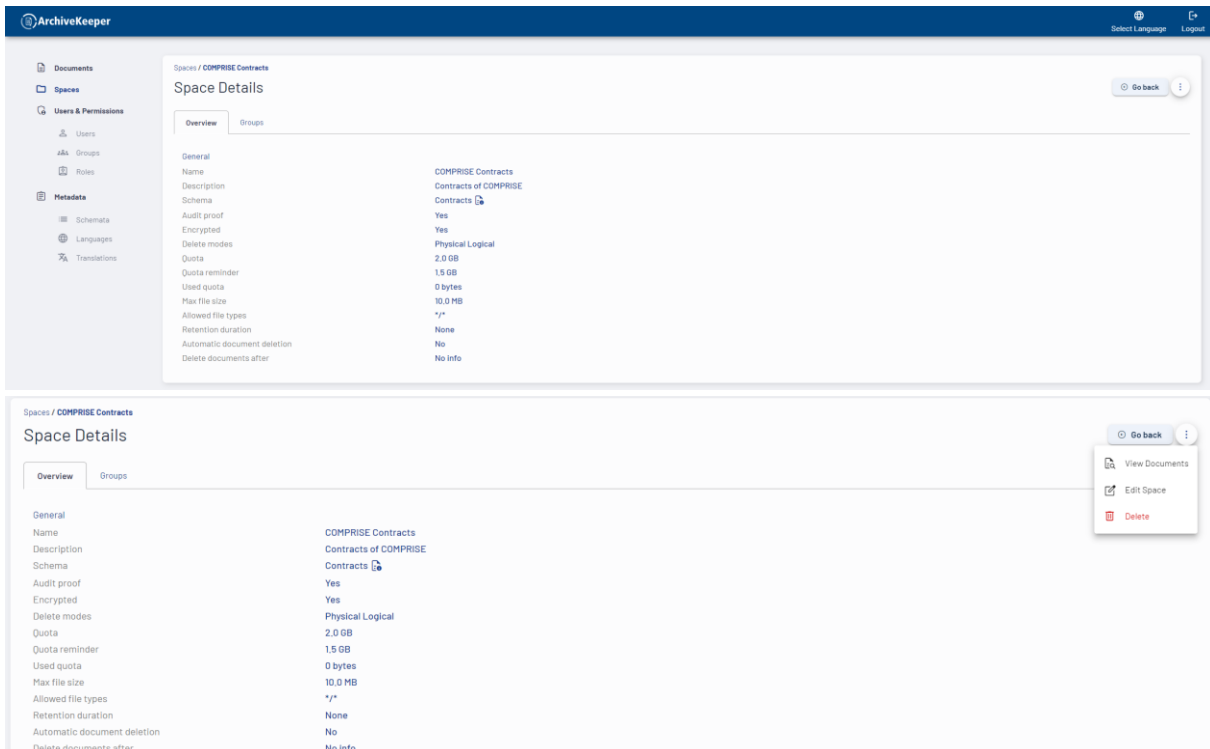
- The Retention period can no longer be changed at a later date in order to maintain traceability.
- It is also not possible to change the revision safety (audit-proof), as this would enable manipulation.
- The schema change is also only possible to a limited extent, as all previous metadata must also be available in the new schema.
 - With the new schema, only changes to the display settings can be made to the metadata that was also contained in the previous schema
 - There are no restrictions for metadata that was not included in the schema already in use.
 - The exact procedure for this can be found under [Metadata schema](#).

6.2.1.3 Document space details



Name	Description	Size	Actions
COMPRISE Contracts	Contracts of COMPRISE	10.0 MB	

The view of the document space details in the administration differs from that of the standard user. In the overview, you can switch directly to the metadata schema details of the schema used. Further actions are available in the details via the dots in the top right-hand corner. There is also the "Groups" tab where the assigned groups can be managed.

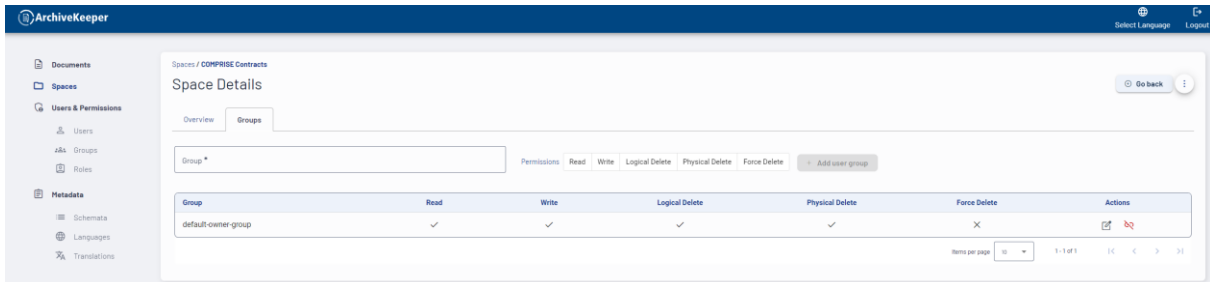


The screenshot shows the 'Space Details' page for 'COMPRISE Contracts' in the ArchiveKeeper interface. The left sidebar contains navigation links for Documents, Spaces, Users & Permissions, and Metadata. The main content area is divided into 'Overview' and 'Groups' tabs. The 'Overview' tab is active, displaying a table of space properties.

General	
Name	COMPRISE Contracts
Description	Contracts of COMPRISE
Schema	Contracts
Audit proof	Yes
Encrypted	Yes
Delete modes	Physical Logical
Quota	2.0 GB
Quota reminder	1.5 GB
Used quota	0 bytes
Max file size	10.0 MB
Allowed file types	*/*
Retention duration	None
Automatic document deletion	No
Delete documents after	No info

On the right side of the 'Overview' tab, there is a 'Go back' button and a menu with options: View Documents, Edit Space, and Delete.

6.2.1.3.1 Groups



The screenshot shows the 'Groups' tab of the 'Space Details' page. It features a search bar for groups and a table listing the groups and their permissions.

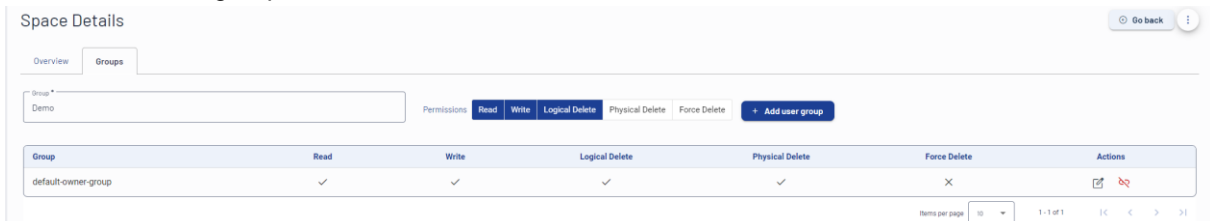
Group	Read	Write	Logical Delete	Physical Delete	Force Delete	Actions
default-owner-group	✓	✓	✓	✓	✗	

At the top of the table, there is a search bar labeled 'Group *' and buttons for 'Permissions', 'Read', 'Write', 'Logical Delete', 'Physical Delete', 'Force Delete', and 'Add user group'.

The Groups tab of the document space details contains all groups and their rights. New groups can be added or existing groups can be edited or deleted using actions.

For the administration of groups see: [Groups](#)

6.2.1.3.1.1 Add group



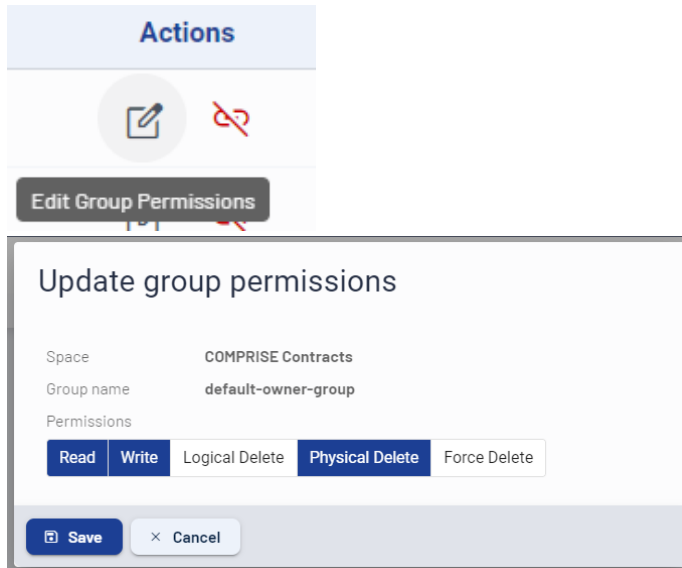
This screenshot shows the 'Groups' tab with the search bar filled with the text 'Demo'. The table below shows the 'default-owner-group' with its permissions.

Group	Read	Write	Logical Delete	Physical Delete	Force Delete	Actions
default-owner-group	✓	✓	✓	✓	✗	

In the Group field, you can search for the corresponding group (which has not yet been assigned to the document space).

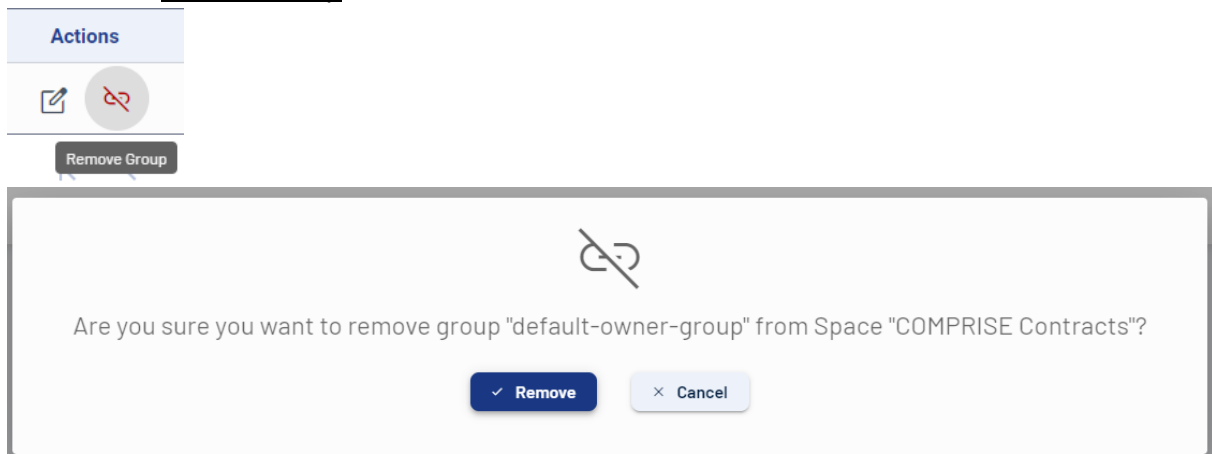
The specific rights can be assigned by selecting and deselecting.

6.2.1.3.1.2 Edit group



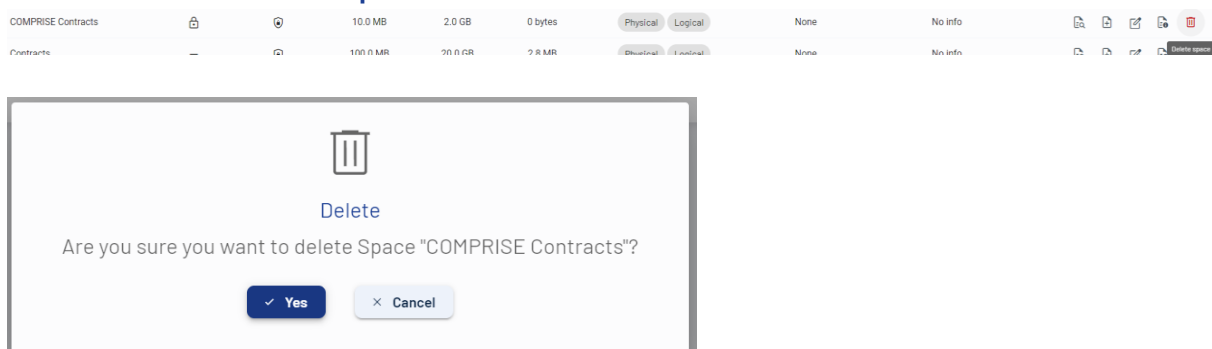
The rights can be adjusted in the "Edit group rights" pop-up by selecting/deselecting them.

6.2.1.3.1.3 Remove Group



Groups can be removed from the document space using the "Remove Space" action. When removing, an additional pop-up appears to confirm the action.

6.2.1.4 Delete document space



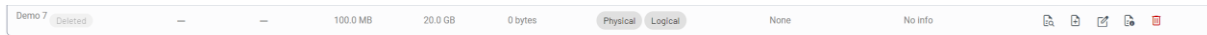
Document spaces can only be deleted if no groups are assigned to the document space. If you want to delete a document space, the assigned groups must therefore be removed first.

When deleting the document space, a distinction is made depending on whether the document space is audit-proof or not.

6.2.1.4.1 Non-auditable document space

The document space is initially only "marked for deletion" and the contents of the document space can still be viewed during this time.

After 2 days, the storage is deleted. All files in the storage, documents, revisions and audit logs are deleted. Only the document space object itself is not deleted, but is set to the status "Deleted".



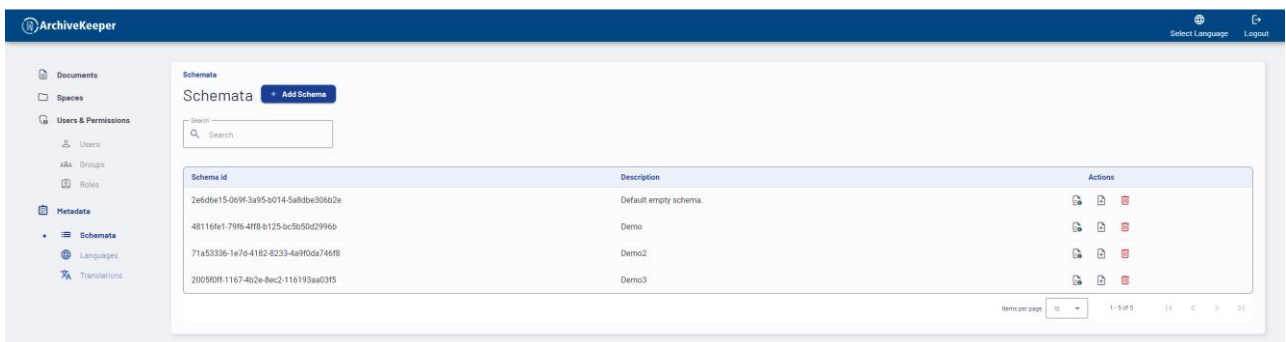
This non-auditable document space is marked for deletion.

6.2.1.4.2 Audit-proof document space

Works in the same way as deleting a non-auditable document space. However, the evidence and reduced daily hashes of the document space (or its revisions) are also physically deleted here.

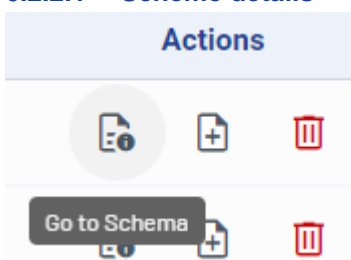
In addition, all reduced revisions (insensitive remnants from the physical deletion) are also removed.

6.2.2 The metadata schema



The entire schemas can be managed under Metadata Schemata.

6.2.2.1 Scheme details



The actions can be used to access detailed information about a scheme.

Schemata / Contracts

Schema Details

Go back

Overview

General

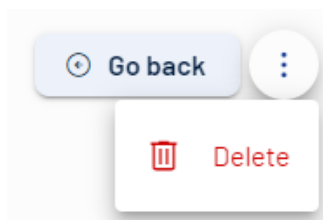
Schema id: 27e4c201-4364-4763-93dd-093d7116b2e7

Description: Contracts

Key	Position	Source	Value Type	Actions
Cat	0	USER_DEFINED	STRING	
filename	1	DOCUMENT	STRING	
CustomerNr	2	USER_DEFINED	STRING	
Information	3	USER_DEFINED	STRING	
ValidFrom	4	USER_DEFINED	LOCAL_DATE	
ValidTo	5	USER_DEFINED	LOCAL_DATE	
createdAt	6	DOCUMENT	UTC_DATETIME	

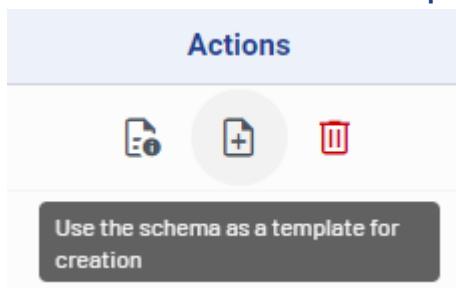
The individual schema fields and their settings can be seen in the detailed view.

The translations of the individual fields can be edited. Other setting changes are not possible.



Only deletion is possible as an action. This is only permitted if no document space has been assigned to the schema.

6.2.2.2 Create schema with template



The Schema function can be used as a template for creation via the actions.

The template function is particularly helpful if a new schema is to be assigned to a document space. This is because all fields of the old schema must also be included in the new schema and the encoding of these fields must remain unchanged. New fields can be added as required. This means that the template can be used for this application, new fields can be added or the display settings of the existing fields can be changed (this is permitted).

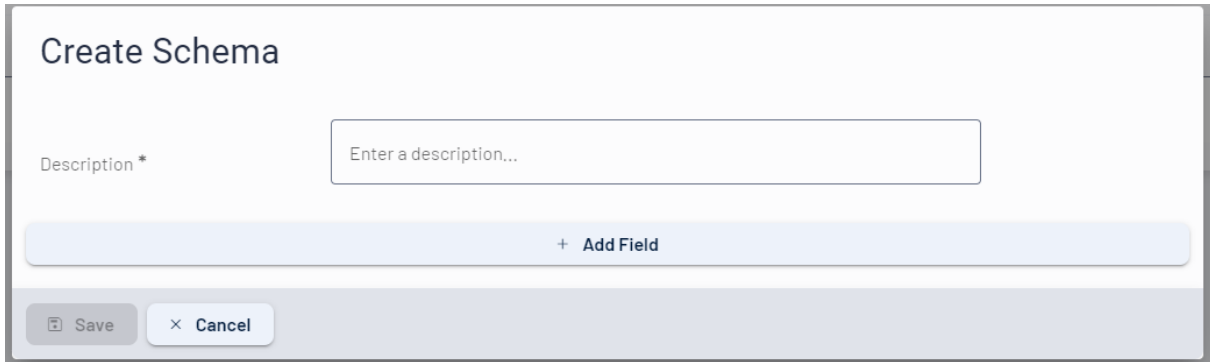


With this function, all fields of the selected schema are now visible and can be edited or deleted (note if this new schema is to replace the old one).

New fields can be added.

The description should be adapted to better distinguish the new scheme.

6.2.2.3 Add Schema



A new schema can be created using the "Add schema" button.

A description must be defined for each schema (this can be equated with a name).

The individual metadata fields can now be added via "Add field".

Create Schema Field

Key *

Key Translation

Choose Translation Content

+

Source *

USER_DEFINED

▼

Value Type *

STRING

▼

Position

Automatic

Audit Proof

Yes

No

Encrypted

Yes

No

Indexed

Yes

No

Retain deleted data

Yes

No

Constraints

▼

Display Options

▼

Save

× Cancel

Clicking on "Add field" opens a separate pop-up in which the individual settings for the respective metadata field can be made.

6.2.2.3.1 Field

A unique name for the schema must be defined for the field.

6.2.2.3.2 Key translation


It is possible to define a translation for the characteristic (see [Translations](#)). In this field, you can search for existing translations or add a new translation.

Example: The field is labeled Cat and the translation Cat is added as a translation.

Create Schema Field

Key *

Key Translation
(Translation Selected)



Source *

USER_DEFINED ▼

Create Translation

Name *

Language

English ▼

Category

⊖

Language

Deutsch ▼

Kategorie

⊕ ⊖

Save

Cancel

As shown in this image, the translation Cat will display the name Category in the English language and the name Kategorie in the German language. This means that if a user has set English as the language, the name Category will be displayed for this field when uploading documents or viewing the metadata of a document.



In this picture you can see how the field Cat with the translation Cat is displayed to the user with the German language as category.

6.2.2.3.3 Source

Source *

USER_DEFINED ▼

Value Type *

DOCUMENT

USER_DEFINED ✓

There are two possible types of metadata fields DOUCMENT and USER_DEFINED.

USER_DEFINED are fields that are created individually by the user and allow all configuration options. **DOCUMENT** refers to metadata fields that have already been defined (general metadata). The possible settings for this metadata are limited.

For fields of this type, it is possible to define the display settings, revision safety, etc. according to your own requirements.

Create Schema Field

Key *	<div>Enter a unique key... ▼</div>
Key Translation	
Source *	
Value Type *	
Position	

As these are existing fields, it is not possible to define your own characteristic name in the DOCUMENT function; instead, the characteristic must be selected from a drop-down list.

Create Schema Field

Key *	<div>filename ▼</div>
Key Translation	<div>Choose Translation Content +</div>
Source *	<div>DOCUMENT ▼</div>
Value Type *	<div>STRING ▼</div>
Position	<div>Automatic</div>
Audit Proof	<div>Yes No</div>
Encrypted	<div>Yes No</div>
Indexed	<div>Yes No</div>
Retain deleted data	<div>Yes No</div>

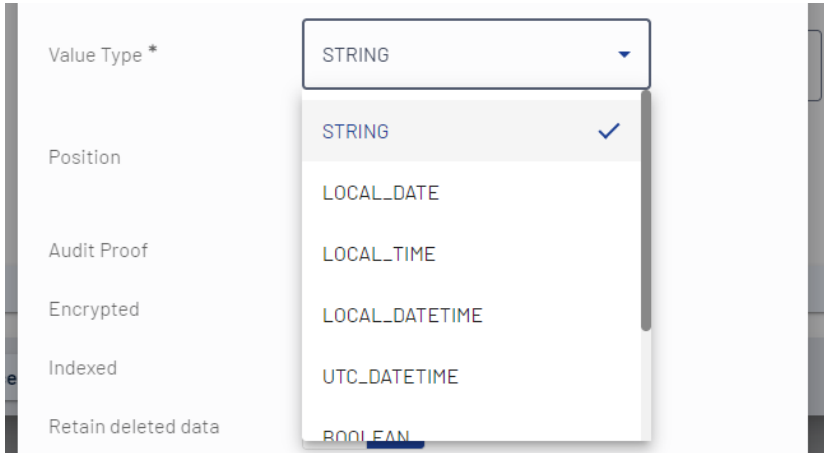
Constraints ^

Read-only	<div>Yes No</div>
Mandatory	<div>Yes No</div>

Here the characteristic Filename with source DOCUMENT as an example. This field cannot be encrypted as the file name is required for various operations. In addition, only read access is possible, users cannot change the file name when uploading.

However, you can individually define whether the field should be retained when it is deleted or whether it should be audit-proof.


6.2.2.3.4 Value type



Various value types can be defined for the metadata field. This influences the possible entries and further setting options

- String: Alphanumeric characters
- BOOLEAN: True/False values
- Integer: Numerical values
- Decimal: Numerical values with decimal places
- Other date values and time values

6.2.2.3.5 Position



The position influences the sorting (always starts with 0, display order of the metadata in the details of the documents) When a further characteristic is added, the position is automatically increased by one. It is therefore not necessary to make changes to the position unless a different sorting is required.

6.2.2.3.6 Further definitions

Audit Proof	Yes	No
Encrypted	Yes	No
Indexed	Yes	No
Retain deleted data	Yes	No

If a metadata field is defined as audit-proof, this is taken into account in the evidence and revision assurance processes. After the document has been deleted, remnants remain for tracking the revision control.

With Encrypted, a metadata field is stored in encrypted form. However, encrypting a metadata field means that it can no longer be searched for.

Indexed must be selected if the metadata field is to be searchable.

If Retain deleted data is active, the field is retained in full even after deletion.

6.2.2.3.7 Constraints

Constraints

Read-only

Yes No

Mandatory

Yes No

Minimum length

0

characters

Maximum length

0

characters

Accepted value
(No Translation Sel.)

Choose Translat

+

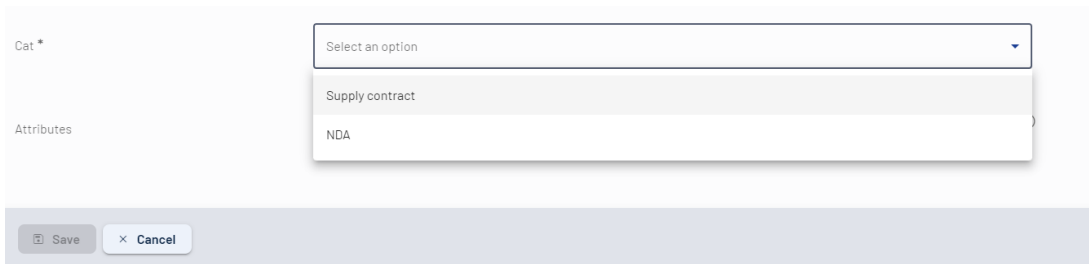
🔗

+

Under Constraints you can manage whether the metadata field can only be used read-only or whether it should be a mandatory field (must be specified when uploading documents)

Furthermore, restrictions are possible when entering the field:

- Minimum length: Min. length of input
- Maximum length: Max. Length of the input
- Allowed values: If permitted values are defined, the user can select the defined values from a drop-down list when uploading



This screen shows the document upload. When creating the schema, report, information, log, invoice and other were defined as permitted values for the category. The user can now choose from these values when uploading.


6.2.2.3.8 Display options



In the details page: If Yes, the metadata field is displayed in the document details

In search results: If Yes, it will be displayed in the search results

Filterable: If yes, it can be searched for under "Advanced filters".

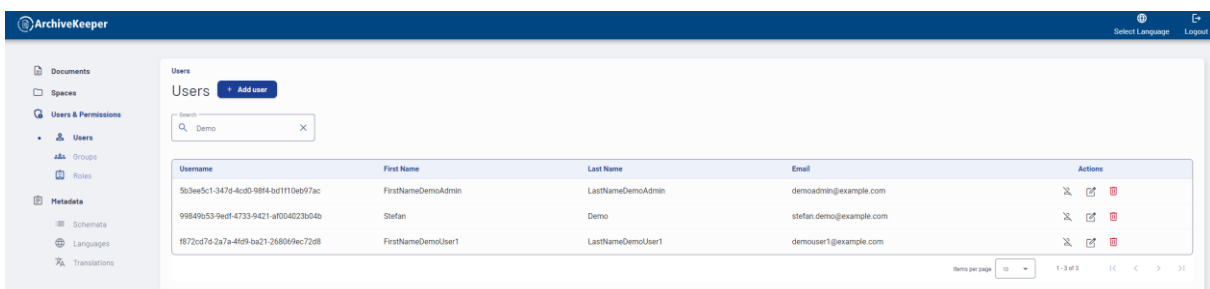


This is particularly useful for fields that have defined permitted values or for date and time formats.

Search by text: If Yes, you can search for the field content in the normal search field.



6.2.3 Users



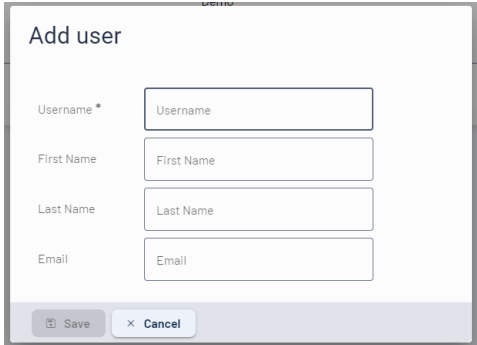
Username	First Name	Last Name	Email	Actions
5b3ee5c1-347d-4cd9-9894-bd11f0e697ac	FirstNameDemoAdmin	LastNameDemoAdmin	demoadmin@example.com	[Edit] [Delete] [Add]
99849b53-9edf-4733-9421-af04023804b	Stefan	Demo	stefan.demo@example.com	[Edit] [Delete] [Add]
1b72cd74-2a7a-4d69-ba21-268069ec72d8	FirstNameDemoUser1	LastNameDemoUser1	demouser1@example.com	[Edit] [Delete] [Add]

New users can be added and existing users can be managed under Users.

The search function makes it easy to find existing users.

6.2.3.1 Add user

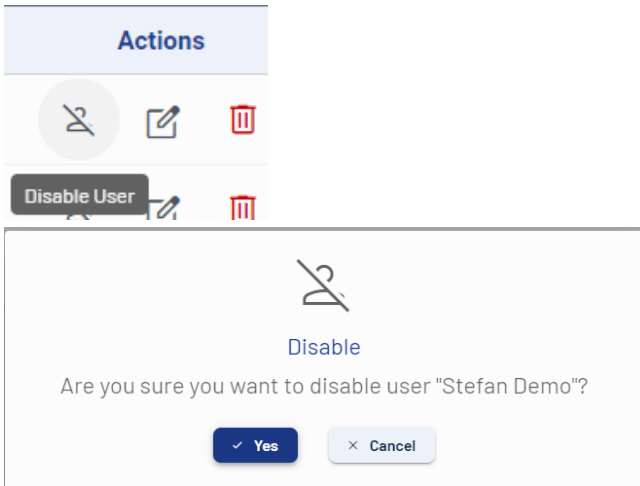
Additional users can be saved in ArchiveKeeper using the "Add user" button.



The "Add user" form contains four input fields: "Username *" (required), "First Name", "Last Name", and "Email". Below the fields are "Save" and "Cancel" buttons.

When adding, the user's basic data must be added.

6.2.3.2 Deactivate user

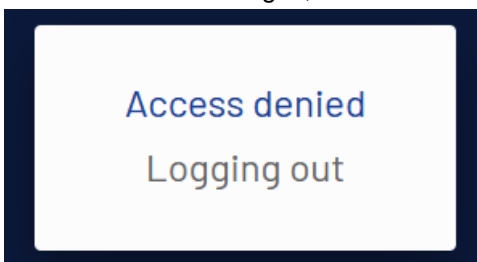


The interface shows a list of users with an "Actions" menu. The "Disable User" button is highlighted. A confirmation pop-up is displayed with the text "Are you sure you want to disable user 'Stefan Demo'?" and "Yes" and "Cancel" buttons.

The user can be deactivated in the actions. The action must be confirmed again in the pop-up.

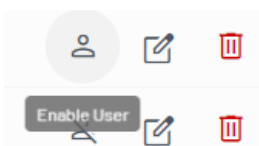
Deactivated users are still present in ArchiveKeeper, but no longer have access to ArchiveKeeper.

If this user wants to log in, the information "Access denied" appears on the login screen.



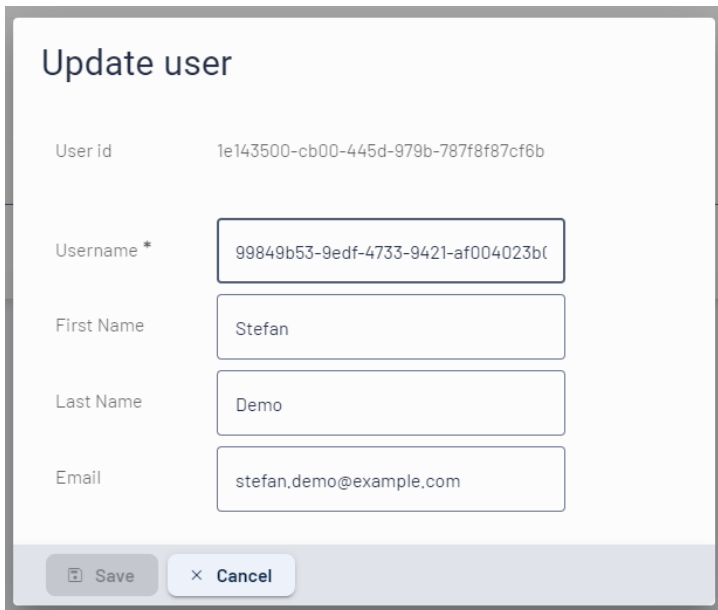
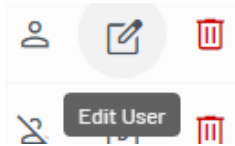
The "Access denied" screen displays the text "Access denied" in blue and "Logging out" in grey.

Deactivated users can be reactivated in ArchiveKeeper at any time



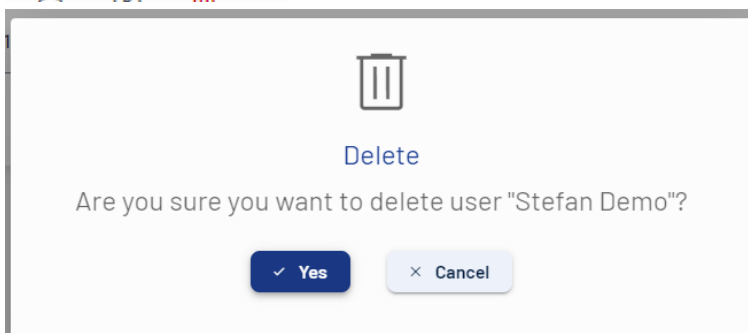
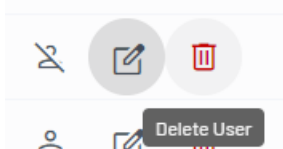
The interface shows a list of users with an "Actions" menu. The "Enable User" button is highlighted.

6.2.3.3 Edit user

A form titled 'Update user' with a light gray background. It contains the following fields: 'User id' with the value '1e143500-cb00-445d-979b-787f8f87cf6b', 'Username *' with the value '99849b53-9edf-4733-9421-af004023b...', 'First Name' with the value 'Stefan', 'Last Name' with the value 'Demo', and 'Email' with the value 'stefan.demo@example.com'. At the bottom, there are two buttons: 'Save' and 'Cancel'.

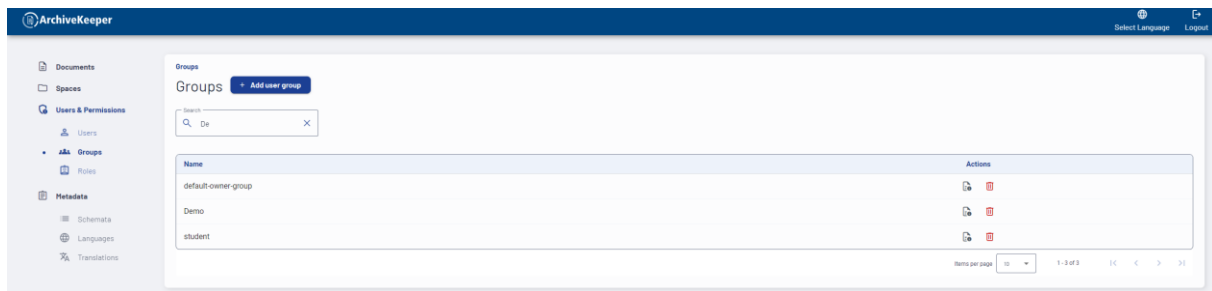
The Edit action can be used to adjust the information for a user.

6.2.3.4 Delete user

A confirmation dialog box with a light gray background. It features a trash can icon at the top, followed by the word 'Delete' in blue. Below this, the text asks: 'Are you sure you want to delete user "Stefan Demo"?'. At the bottom, there are two buttons: 'Yes' (with a checkmark icon) and 'Cancel' (with an 'x' icon).

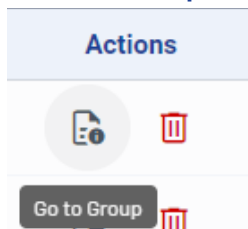
Users can also be deleted again. This must also be confirmed again. In contrast to deactivation, the user is deleted from the system.

6.2.4 Groups

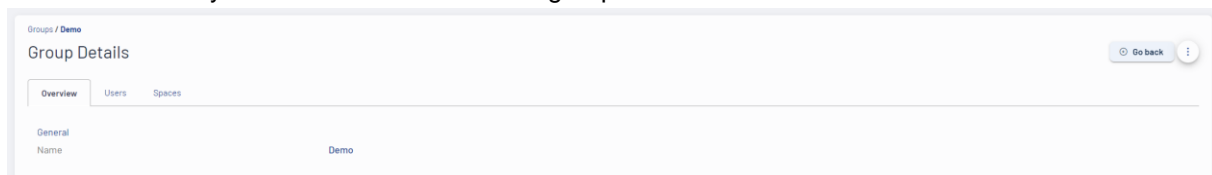


Existing groups can be managed and new groups added under Groups.
The search function makes it easy to find existing groups.

6.2.4.1 Group details



The actions take you to the detailed view of a group.

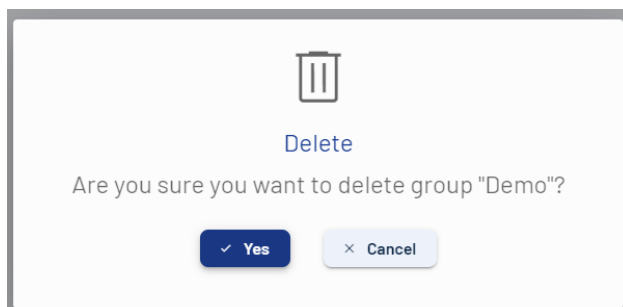


There are three tabs to choose from (Overview, Users and Document spaces) and two actions that can be selected via the menu (three dots).

6.2.4.1.1 Edit

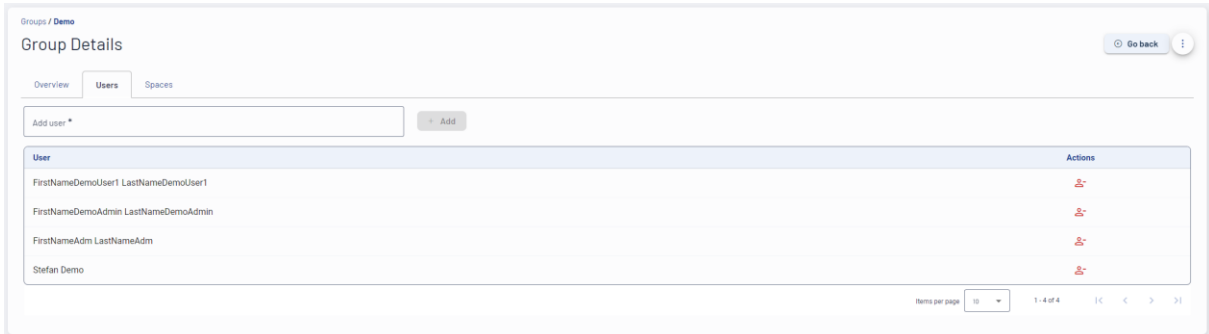
The group name can be changed when editing.

6.2.4.1.2 Delete



This allows you to delete the group. A pop-up appears in which the deletion must be confirmed.

6.2.4.2 Users



Groups / Demo

Group Details

Overview Users Spaces

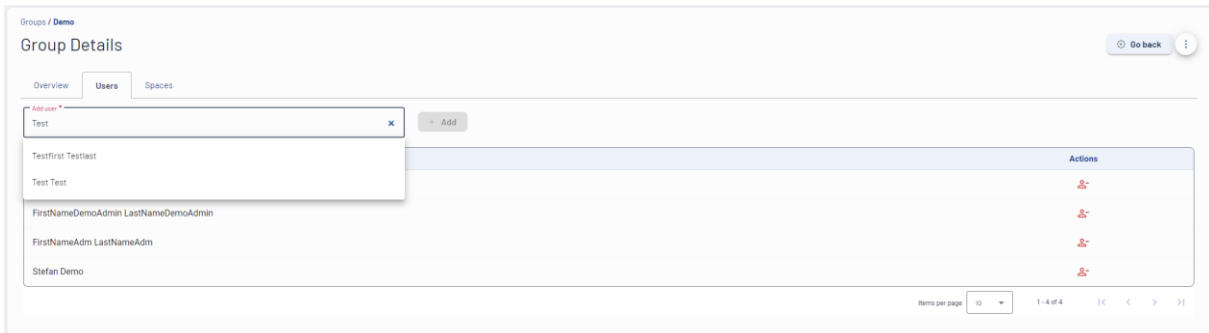
Add user *

Add

User	Actions
FirstNameDemoUser1 LastNameDemoUser1	
FirstNameDemoAdmin LastNameDemoAdmin	
FirstNameAdm LastNameAdm	
Stefan Demo	

Items per page 10 1 - 4 of 4 |< < > >|

In the Users tab, existing users can be removed from the group and new users can be added.



Groups / Demo

Group Details

Overview Users Spaces

Add user *

Test

Testfirst Testlast

Test Test

FirstNameDemoAdmin LastNameDemoAdmin

FirstNameAdm LastNameAdm

Stefan Demo

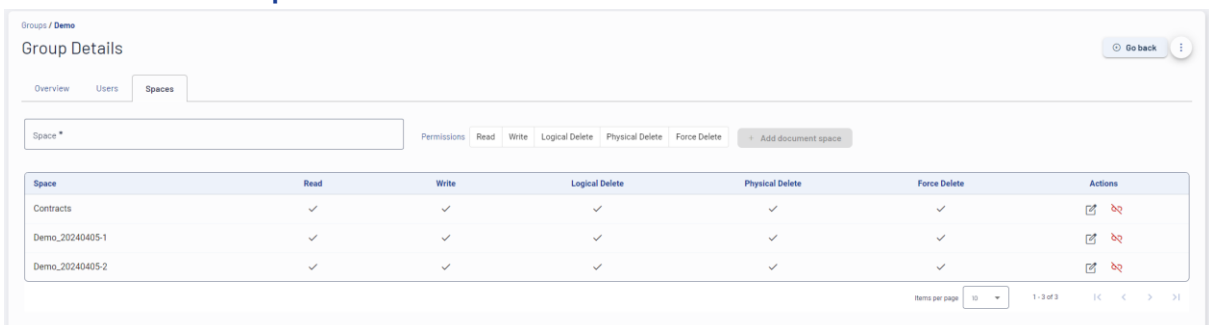
Add

User	Actions
FirstNameDemoAdmin LastNameDemoAdmin	
FirstNameAdm LastNameAdm	
Stefan Demo	

Items per page 10 1 - 4 of 4 |< < > >|

The desired user can be searched for and added to the group via the input field.

6.2.4.3 Document spaces



Groups / Demo

Group Details

Overview Users Spaces

Space *

Permissions Read Write Logical Delete Physical Delete Force Delete Add document space

Space	Read	Write	Logical Delete	Physical Delete	Force Delete	Actions
Contracts	✓	✓	✓	✓	✓	
Demo_20240405-1	✓	✓	✓	✓	✓	
Demo_20240405-2	✓	✓	✓	✓	✓	

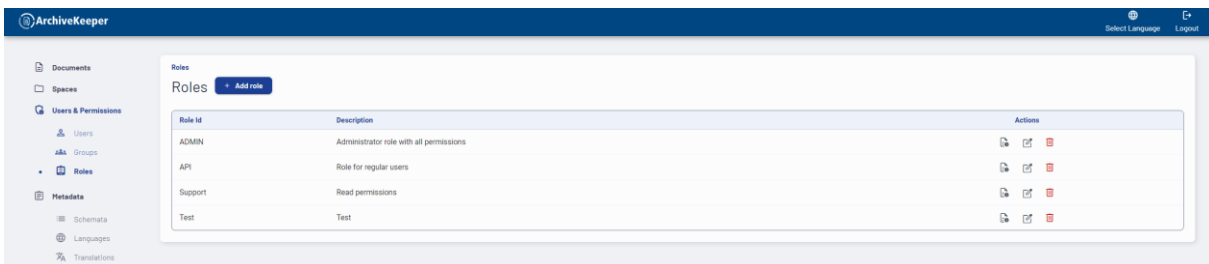
Items per page 10 1 - 3 of 3 |< < > >|

Similar actions are possible under spaces as when editing the groups in a document space (see [Document space](#)).

The only difference is that the document spaces are managed for the specific group and not vice versa. The desired document space can be added via the input field and the corresponding rights assigned. (see [authorization concept](#))

For existing document spaces, the rights for the group can be adjusted or the document space can be removed.

6.2.5 Roles



ArchiveKeeper

Select Language Logout

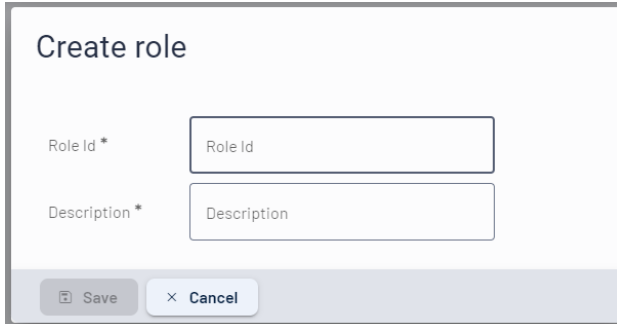
Documents Spaces Users & Permissions Roles Metadata Schemata Languages Translations

Roles Add role

Role Id	Description	Actions
ADMIN	Administrator role with all permissions	
API	Role for regular users	
Support	Read permissions	
Test	Test	

Existing roles can be edited and new roles added under Roles.

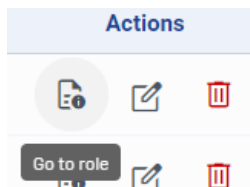
6.2.5.1 Create role



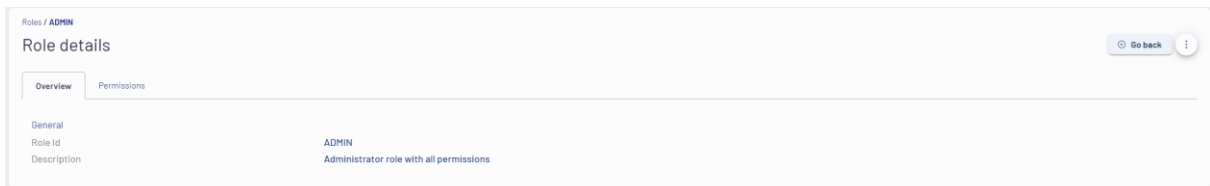
The 'Create role' form contains two input fields: 'Role Id *' and 'Description *'. Both fields have placeholder text matching their labels. At the bottom, there are two buttons: 'Save' and 'Cancel'.

When creating a role, initially only the unique name (ID) and the description need to be defined. The authorizations are assigned in the role details.

6.2.5.2 Roll details

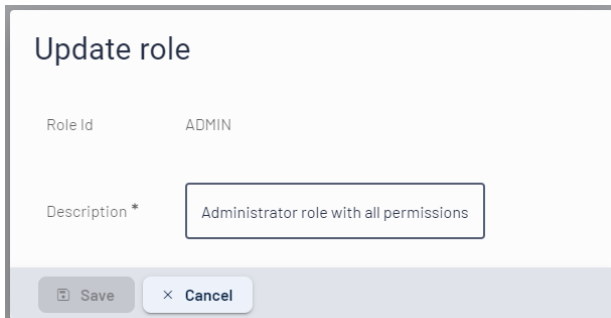


6.2.5.2.1 Overview

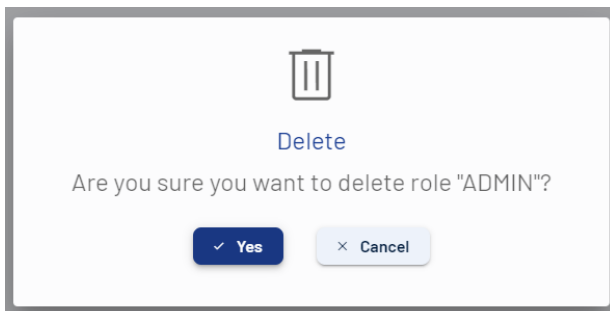


The 'Role details' overview tab shows the role 'ADMIN' with its ID and description. The description is 'Administrator role with all permissions'. There is a 'Go back' button in the top right corner.

The ID and description of the role can be seen in the overview tab. The description can be edited via the menu (ID cannot be changed) or the role can be deleted.



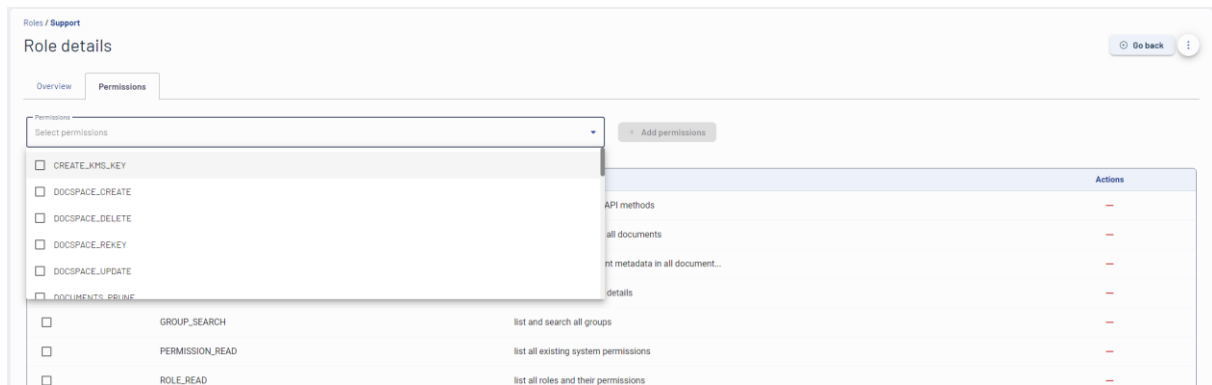
The 'Update role' form shows the role 'ADMIN' with its ID and description. The description is 'Administrator role with all permissions'. There are 'Save' and 'Cancel' buttons at the bottom.



The 'Delete' dialog asks 'Are you sure you want to delete role "ADMIN"?'. It has 'Yes' and 'Cancel' buttons.

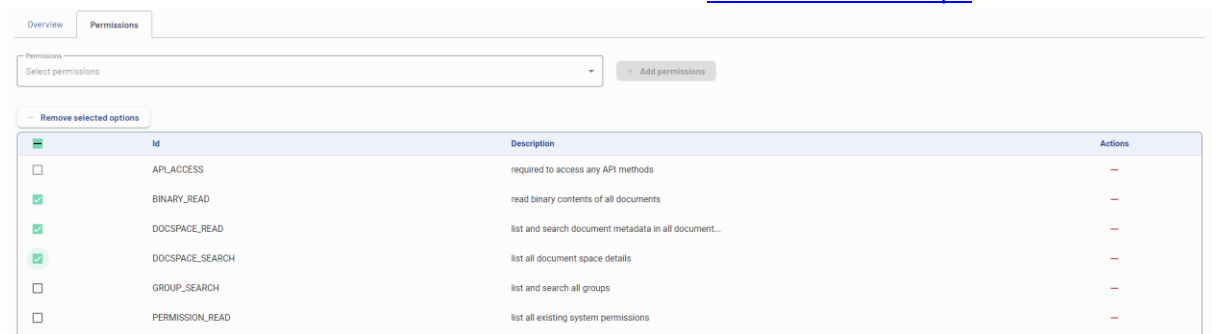
The deletion of a role must also be confirmed

6.2.5.2.2 Permissions



The existing authorizations can be seen in the Permissions tab and further authorizations can be selected via the Permission field.

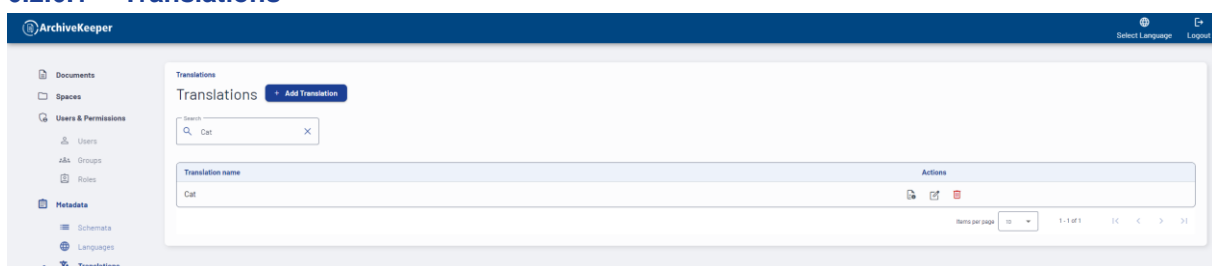
Details on the individual authorizations can be found under [Authorization concept](#).



Permissions can be removed individually via actions or collectively by selecting the desired permission via checkboxes and removing them from the role via "Remove selected options".

6.2.6 Translations

6.2.6.1 Translations

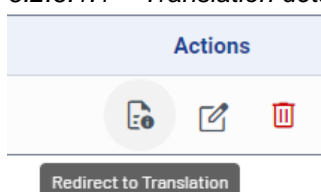



Under Translations, new translation content can be added and existing translations can be edited or deleted.

The search function can be used to search for existing translations.

The translations are used for the translation of metadata schemas.

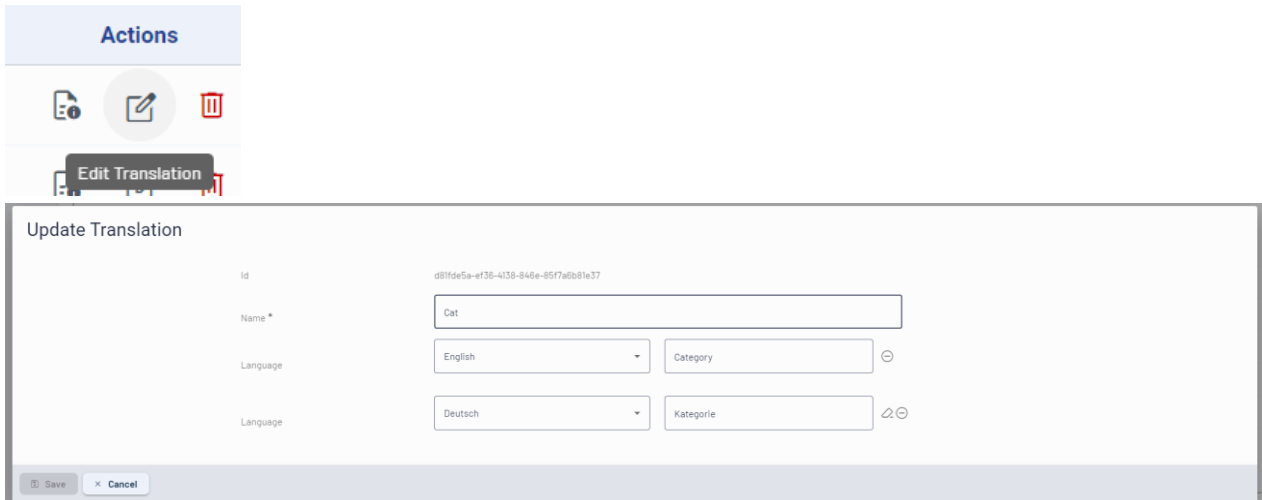
6.2.6.1.1 Translation details





The translation details show the ID, name and the individual translations for each language. The translations can be edited or the translation deleted via the menu.

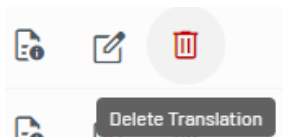
6.2.6.1.2 Edit translation



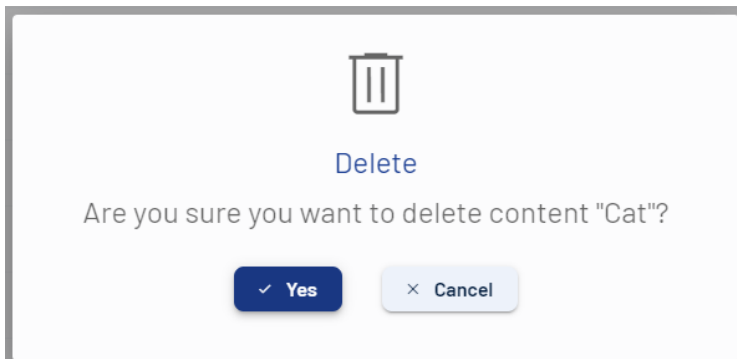
When editing, the translation name can be changed, and the translations of the individual languages and new languages for translations can be added.

The available languages can be managed under the Languages menu (see [Languages](#))

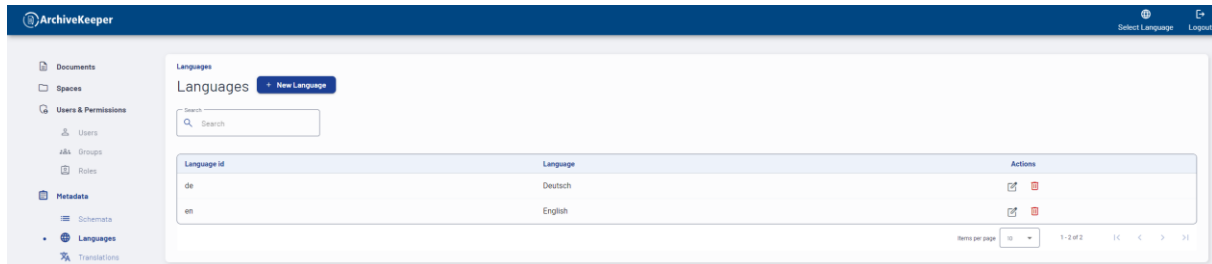
6.2.6.1.3 Delete translation



Translations can only be deleted if they are not used in any schema.

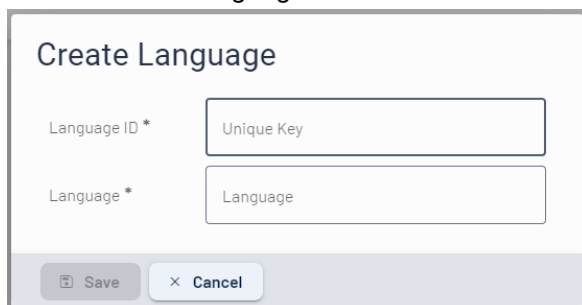


6.2.6.2 Languages



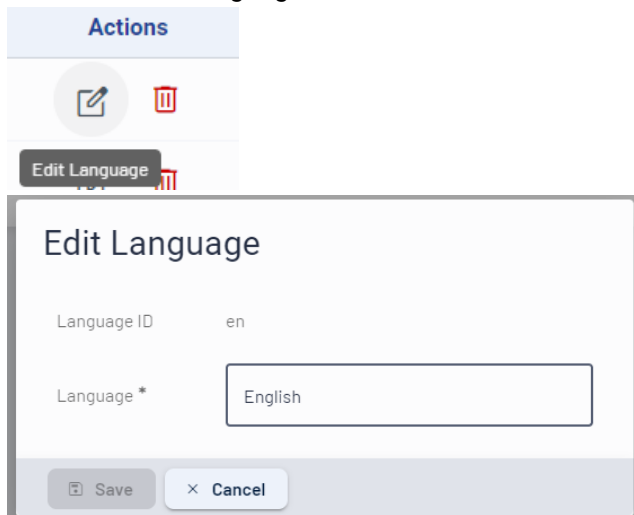
Languages can be added or managed under Languages. These languages are then available in the individual translations (Translations menu).

6.2.6.2.1 Add language



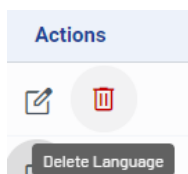
When adding a language, a unique ID and the name of the language must be defined. e. g. ID = de-at and language = German and ID = de-ch and language = German.

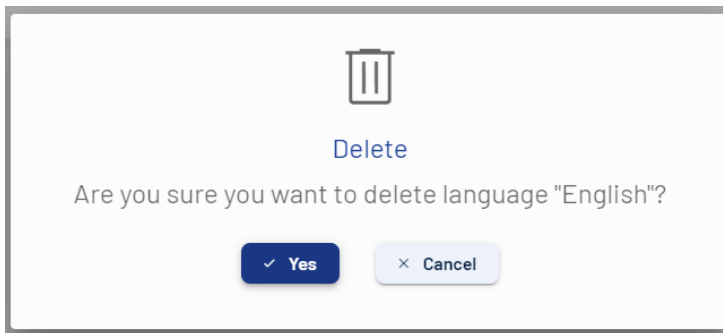
6.2.6.2.2 Edit language



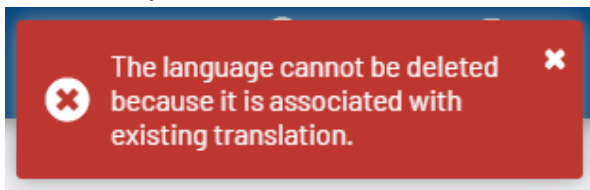
When editing, only the language name can be changed but not the ID.

6.2.6.2.3 Delete language





It is possible to delete a language via the actions. However, only languages for which there are no translations yet can be deleted.



Error message as the selected language is already used for translations.

COMPRISE GmbH
Wiedner Hauptstraße 76/2
1040 Wien
Austria, Europe

<https://www.comprise.world>
info@comprise.world

Copyright

© 2024 All rights reserved, including the right to reprint extracts, to make electronic or photomechanical copies and to analyse by means of electronic data processing.